COMPUTATIONAL RESEARCH in BOSTON and BEYOND SEMINAR

Aspects of Robustness and Representation in Machine Learning

STEFANIE JEGELKA

Massachusetts Institute of Technology

ABSTRACT:

Reliability of machine learning methods includes many facets. One aspect are robust, stable algorithms. Another one is a better theoretical understanding of properties of currently popular models. In this talk, I will show recent work on both these directions.

First, we address robustness for black-box optimization with Gaussian Processes (GPs). GP-based methods have become popular tools for sequentially optimizing an unknown function that is expensive to evaluate, with applications in robotics, hyperparameter tuning, recommender systems and environmental monitoring. In such applications, robust, stable solutions are of interest for several reasons: the underlying functions during optimization and implementation stages are different, or one seeks an entire region of good inputs rather than only a single point. We formalize this by allowing the query point to be adversarially perturbed, and require the function value to remain as high as possible even after this perturbation. Standard GP optimization approaches can fail in this setting. We provide a new, confidence-bound based algorithm, and establish lower and upper bounds on the required number of samples to find a near-optimal point.

Second, we explore the representational power of ResNet, a popular recent neural network architecture that augments the network with a parallel identity mapping. While classical results address wide, shallow networks, we ask how narrow a deep ResNet can be to still allow universal approximation. Our results show that one hidden unit is enough, in sharp contrast to fully connected networks.

This talk is based on joint work with Ilija Bogunovic, Jonathan Scarlett, Volkan Cevher and Hongzhou Lin.

FRIDAY, NOVEMBER 2, 2018
1:00 PM – 2:00 PM
Building 32, Room 155
STATA

Pizza and beverages will be provided.

http://math.mit.edu/crib/

Massachusetts Institute of Technology