College of Arts and Sciences
Department of Mathematics
University of South Carolina

Math Colloquium

PDE Principled Trustworthy Deep Learning Meets Computational Biology

Dr. Bao Wang, PIC Assistant Adjunct Professor
Department of Mathematics, UCLA

Friday
December 13th
4:00 PM
LeConte 405

Deep learning achieves tremendous success in image and speech recognition and machine translation. However, deep learning is not trustworthy.

1. *How to improve the robustness of deep neural networks?* Deep neural networks are well known to be vulnerable to adversarial attacks. For instance, malicious attacks can fool the Tesla's self-driving system by making a tiny change on the scene acquired by the intelligence system.

2. *How to compress the high-capacity deep neural networks efficiently without loss of accuracy?* It is notorious that the computational cost of inference by the deep neural network is one of the major bottlenecks for applying them to mobile devices.

3. *How to protect the private information that is used to train the deep neural network?* Deep learning-based artificial intelligence systems may leak the private training data. Fredrikson et al. recently shown that a simple model-inversion attack can recover the portraits of the victims whose face images are used to train the face recognition system.

In this talk, I will present some recent work on developing PDE principled robust neural architecture and optimization algorithms for robust, accurate, private, and efficient deep learning. I will also present some potential applications of the data-driven approach for bio-molecule simulation.

UNIVERSITY OF SOUTH CAROLINA