SCHOOL OF NATURAL SCIENCES

# SEMINAR SERIES

## PDE-Principled Trustworthy Deep Learning Meets Computational Biology

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 self-driving system by making a tiny change on the scene acquired by the intelligence system. 2. *How to compress high-capacity deep neural networks efficiently without loss of accuracy*? It is notorious that the computational cost of inference by deep neural networks is one of the major bottlenecks for applying them to mobile devices. 3. *How to protect the private information that is used to train a deep neural network*? Deep learning-based artificial intelligence systems may leak the private training data. Fredrikson et al. recently showed 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 and computer-aided drug design.

| **Tuesday 2/11/2020** | **3:00pm - 4:30pm** | **Granite Pass, Rm. 135** | For more information, contact: Professor Mayya Tokman at mtokman@ucmerced.edu |
|---|---|---|---|


## Bao Wang

Department of Mathematics
University of California, Los Angeles


I am a postdoc at Department of Mathematics of UCLA, under the mentorship of Professors Andrea L. Bertozzi and Stanley J. Osher. My research interest lies in an synergistic integration of machine learning with first principle-based approaches. I work on developing first-principle inspired conceptually simple, computationally efficient and theoretically principled optimization and sampling algorithms and novel architectures to pursue robust, accurate, private, and data-efficient deep learning. Also, I integrate advanced deep learning algorithms into the classical first principle-based models to advance molecular-scale modeling and computation of the biological systems. I received my Ph.D. degree in Applied Mathematics from the Michigan State University.