Curriculum Vitae

Yuancheng Xu
Email: ycxu@umd.edu
Website: https://yuancheng-xu.github.io/

Education

University of Maryland, College Park
Ph.D. student in Applied Mathematics & Statistics, and Scientific Computation *2020-2025 (expected)*
Advisor: Prof. Furong Huang (Computer Science)

Southern University of Science and Technology, China *2016-2020*
B.S. in Mathematics and Applied Mathematics
GPA 3.94/4.00 (1/909)
Summa Cum Laude (1%)

New York University *Spring, 2019*
Visiting Student at the Courant Institute of Mathematical Sciences
GPA 4.0/4.0

Research Interests

- Robustness of machine learning models against domain shifts and adversarial attacks
- Developing computational approaches to enhance the fairness in machine learning
- Data Condensation
- Understanding privacy, robustness and fairness problems in large language models

Publications and Preprints

1. **Yuancheng Xu**, Yanchao Sun, Micah Goldblum, Tom Goldstein, Furong Huang. "Exploring and Exploiting Decision Boundary Dynamics for Adversarial Robustness". In *International Conference on Learning Representations (ICLR)*, 2023.

2. Mucong Ding, **Yuancheng Xu**, Xiaoyu Liu, Tahseen Rabbani, Teresa Ranadive, Tai-Ching Tuan, Furong Huang. "Faster Hyperparameter Search via Calibrated Dataset Condensation". In Submission, 2023.

3. **Yuancheng Xu**, Yanchao Sun, and Furong Huang. "Everyone Matters: Customizing the Dynamics of Decision Boundary for Adversarial Robustness". In *International Conference on Machine Learning (ICML) Workshop on Continuous Time Perspectives in Machine Learning*, 2022.

4. **Yuancheng Xu**, Athanasse Zafirov, R. Michael Alvarez, Dan Kojis, Min Tan, and Christina M. Ramirez. "FREEtree: a Tree-Based Approach for High Dimensional Longitudinal Data with Correlated Features". *Preprint*, 2020.

Research Experience

- **Research Assistant** University of Maryland, College Park

Ph.D. Advisor: Prof. Furong Huang (Computer Science) *June 2020 - Present*

- **Adversarial Robustness of Deep Neural Networks**

  Propose the first framework that directly studies the decision boundary dynamics during training, which can be used to interpret the training of deep neural networks.

  Propose a robust training method that *directly* increases the distances between the decision boundary and data points and prioritizes increasing smaller distances.

- **Fairness in Machine Learning**

  Develop a systematical framework for fairness in the sequential decision-making process problem.

  Design methods for enhancing fairness in NLP and computer vision applications.

- **Research Intern** University of California, Los Angeles

Cross-disciplinary Scholars in Science and Technology (CSST) Program *May – Sept 2019*

Advisor: Prof. Christina Ramirez (Biostatistics)

- **Tree-based Methods for Longitudinal Analysis**

  Propose a tree-based method, FREEtree, for longitudinal data analysis that considers random effects and treatment-time interactions. Compared with previous methods, FREEtree reduces the bias in feature selection by leveraging techniques in clustering and principal component analysis.

  Adapt Weighted correlation network analysis (WGCNA) to longitudinal dataset by using the distance measures of time series such as dynamic time warping (DTW).

- **Research Intern** New York University, Shanghai

Undergraduate Research program *May – Sept 2018*

Advisor: Prof. Sukbin Lim (Neuroscience)

- **Computational Mechanisms for Working Memory**

  Use the theories of differential equations to derive conditions for persistent activity in both parametric and spatial neural networks.

  Simulation of negative derivative feedback control model that attains persistent firing rate in the absence of stimulus using high-performance computing resources.

Awards

Dean's fellowship, University of Maryland, College Park	2020,2021
Summa Cum Laude at Southern University of Science and Technology (10/1000)	2020
China National Scholarship (0.2%, Highest honor of Chinese undergraduate students)	2019
National Mathematical Olympiad (National Second Prize)	2015

Relevant Ph.D. Courses

Scientific Computing I&II, Advanced Numerical Optimization, Foundations of Deep Learning, Numerical Methods for Data Science, Information Theory, Parallel Computing, Natural Language Processing, Differential Geometry, Stochastic Analysis (NYU), Monte-Carlo Method (NYU).