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

My research focuses on **Trustworthy Machine Learning**, including adversarial robustness, fairness, privacy, and interpretability of AI systems. I am particularly interested in automatic search for undesirable behaviors in **foundation models** like large language models and vision-language models.

Publications and Preprints

1. Xiaoyu Liu, Jiaxin Yuan, Bang An, **Yuancheng Xu**, Yifan Yang, Furong Huang. "C-Disentanglement: Discovering Causally-Independent Generative Factors under an Inductive Bias of Confounder". In *Neural Information Processing Systems (Neurips)*, 2023.

2. **Yuancheng Xu**, Chenghao Deng, Yanchao Sun, Ruijie Zheng, Xiyao Wang, Jieyu Zhao, Furong Huang. "Equal Long-term Benefit Rate: Adapting Static Fairness Notions to Sequential Decision Making". In *International Conference on Machine Learning (ICML) workshop on New Frontiers in Adversarial Machine Learning*, 2023.

3. **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.

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

5. **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.

6. **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 Intern** Comcast Applied AI, Washington D.C.

Advisor: Dr. Mahmudul Hasan *June – Sept 2023*

  - Scene-text Understanding via Vision-Language Models

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

Ph.D. Advisor: Prof. Furong Huang (Computer Science) *June 2020 - 2025 (on-going)*

  - Adversarial Robustness of Deep Neural Networks
  - Fairness in Sequential Decision Making
  - Data Efficient Hyperparameter Search

- **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

- **Research Intern** New York University

Undergraduate Research program *May – Sept 2018*

Advisor: Prof. Sukbin Lim (Neuroscience)

  - Computational Mechanisms for Working Memory

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