Leslie Rice

larice@cs.cmu.edu https://leslierice1.github.io/

Education

Carnegie Mellon University Pittsburgh, PA, *August 2018 - May 2023 (anticipated)*
Ph.D. in Computer Science

The University of Texas at Austin Austin, TX, *August 2013 - May 2017*
B.S. in Computer Science
B.S. in Mathematical Sciences, Specialization in Statistics, Probability & Data Analysis

Employment

Carnegie Mellon University Pittsburgh, PA, *August 2018 - Present*
Graduate Research Assistant (Advisor: J. Zico Kolter)
Research on robustness and uncertainty in machine learning.

Google Research Mountain View, CA, *May - August 2022*
Research Intern (Hosts: Cyrus Rashtchian and Da-Cheng Juan)
Research on using knowledge distillation to transfer out-of-distribution generalization.

Bosch Center for Artificial Intelligence Pittsburgh, PA, *May - December 2021*
Machine Learning Research Intern (Host: Wan-Yi Lin)
Research on developing a certified defense against adversarial patch attacks with efficient inference time.

Uber Advanced Technologies Group, *Software Engineer* Pittsburgh, PA, *March 2017 - August 2018*
Developed web-based camera image labeling tools and engineered autolabeling capabilities.

The University of Texas at Austin Austin, TX, *August - December 2016*
Undergraduate Research Assistant (Advisor: Robert A. van de Geijn)
Research on practical, Strassen-like fast matrix multiplication algorithms and performance optimization for the k-nearest neighbors kernel.

Texas Institute for Computational Engineering and Sciences Austin, TX, *June - August 2016*
Moncrief Undergraduate Summer Research Intern (Advisor: Robert A. van de Geijn)
Research on dense matrix multiplication performance optimization using Strassen's algorithm.

Able Lending, *Software Engineer* Austin, TX, *June 2015 - January 2016*
Built data science pipeline for finding small business customers, and developed internal and customer-facing software for managing small business loans.

Applied Research Laboratories at the University of Texas at Austin, *Undergraduate Research Assistant*, Space and Geophysics Lab Austin, TX, *September 2014 - May 2015*
Developed anomaly detection algorithms for geospatial data.

Publications

(Certified!!) Adversarial Robustness for Free!
Nicholas Carlini*, Florian Tramer*, Krishnamurthy (Dj) Dvijotham, Leslie Rice, Mingjie Sun, J. Zico Kolter
International Conference on Learning Representations (ICLR) 2023

Robustness between the worst and average case
Leslie Rice, Anna Bair, Huan Zhang, J. Zico Kolter
Neural Information Processing Systems (NeurIPS) 2021

Overfitting in adversarially robust deep learning
Leslie Rice*, Eric Wong*, J. Zico Kolter
International Conference on Machine Learning (ICML) 2020

Fast is better than free: Revisiting adversarial training
Eric Wong*, Leslie Rice*, J. Zico Kolter
International Conference on Learning Representations (ICLR) 2020

Generating Families of Practical Fast Matrix Multiplication Algorithms
Jianyu Huang, Leslie Rice, Devin A. Matthews, Robert A. van de Geijn
IEEE International Parallel & Distributed Processing Symposium (IPDPS) 2017

*Equal contribution

Workshop Papers

Certified robustness against adversarial patch attacks via randomized cropping
Wan-Yi Lin, Fatemeh Sheikholeslami, Jinghao Shi, Leslie Rice, J. Zico Kolter
ICML 2021 Workshop on Adversarial Machine Learning

Empirical robustification of pre-trained classifiers
Mohammad Sadegh Norouzzadeh, Wan-Yi Lin, Leonid Boytsov, Leslie Rice, Huan Zhang, Filipe Condessa, J. Zico Kolter
ICML 2021 Workshop on Adversarial Machine Learning

Undergraduate Thesis

Performance Optimization for the K-Nearest Neighbors Kernel using Strassen's Algorithm
Leslie Rice
Undergraduate Honors Thesis, The University of Texas at Austin, 2017

Teaching

Carnegie Mellon University, *Graduate Teaching Assistant* Pittsburgh, PA, *August - December 2021*
Deep Learning Systems: Algorithms and Implementation (10-414/714)

Carnegie Mellon University, *Graduate Teaching Assistant* Pittsburgh, PA, *August - December 2018*
Practical Data Science (15-388/688)

The University of Texas at Austin, *Undergraduate Teaching Assistant* Austin, TX, *January - May 2016*
Principles of Computer Systems (CS-439)

Professional Activities

Conference Reviewer
International Conference on Learning Representations (ICLR) 2023
Neural Information Processing Systems (NeurIPS) 2021-2022

Workshop Reviewer
Trustworthy and Socially Responsible Machine Learning at NeurIPS 2022
Adversarial Machine Learning Frontiers at ICML 2022
Robust and Reliable Machine Learning in the Real World at ICLR 2021

Workshop Organizer
Formal Verification of Machine Learning at ICML 2022
A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning at ICML 2021

Ph.D. Admissions Committee Member
Served on the 2021 Ph.D. admissions committee for Carnegie Mellon University's Computer Science Department