Leslie Rice

7121 Gates Hillman Center
Carnegie Mellon University
Pittsburgh, PA 15213

larice@cs.cmu.edu
http://cs.cmu.edu/~larice

Education

Carnegie Mellon University Pittsburgh, PA, *August 2018 - Present*
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

Research Experience

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

Google Research Mountain View, CA, *May - August 2022*
Research Intern (Hosts: Cyrus Rashtchian and Da-Cheng Juan)
Researched methods for robust distillation.

Bosch Center for Artificial Intelligence Pittsburgh, PA, *May - December 2021*
Machine Learning Research Intern (Host: Wan-Yi Lin)
Researched certified defenses against adversarial patch attacks.

The University of Texas at Austin Austin, TX, *August - December 2016*
Undergraduate Research Assistant (Advisor: Robert A. van de Geijn)
Researched 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)
Researched dense matrix multiplication performance optimization using Strassen's algorithm.

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

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
*Equal contribution

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

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

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

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

Industry Experience

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

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.

Invited Talks

Implementing Strassen-Like Fast Matrix Multiplication Algorithms with BLIS (*with Jianyu Huang*), BLIS Retreat, The University of Texas at Austin Austin, TX, *September 2016*

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

Reviewer for ICLR 2023
Reviewer for NeurIPS 2021-2022
Reviewer for NeurIPS 2022 workshop “Trustworthy and Socially Responsible Machine Learning”
Reviewer for the ICML 2022 workshop “Adversarial Machine Learning Frontiers”
Reviewer for the ICLR 2021 workshop “Robust and Reliable Machine Learning in the Real World”
Organizer of the ICML 2022 workshop “Formal Verification of Machine Learning”
Organizer of the ICML 2021 workshop “A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning”
Served on the 2021 PhD admissions committee for the CMU Computer Science Department