Yao Li

Last updated: 27 July, 2020
Github : https://www.github.com/liyao880
LinkedIn: https://www.linkedin.com/in/yao-li-b189574a/
Email: yaoli@email.unc.edu
Phone: (530)-761-8769

EDUCATION

University of California, Davis
Ph.D. in Statistics,
Expected June, 2020 GPA: 4.0/4.0

- **Advisor:** Cho-Jui Hsieh, Thomas C. M. Lee
- **Courses:** Scalable Machine Learning, Computer Vision, Mathematical Statistics, Applied Statistics, Computational Statistics, Statistical Machine Learning

London School of Economics and Political Science (LSE)
Master in Financial Statistics
Oct 2014 - Sep 2015 Grade: Distinction

- **Advisor:** Piotr Fryzlewicz
- **Courses:** Statistical Inference, Time Series, Financial Statistics, Multilevel Modeling, Stochastic Process

Fudan University (211& 985 College in China)
Bachelor of Science in Statistics
Sep 2010 - Jun 2014 GPA: 3.7/4.0

- **Courses:** Probability Theory and Mathematical Statistics, Linear Algebra, Operation Management, Multivariate Statistics, Categorical Data, Financial Management, Accounting

PROFESSIONAL EXPERIENCE

University of California, Davis **Sep 15 - present**
Graduate Teaching Assistant, Department of Statistics

- Responsible for conducting and preparing discussion sections, holding office hours, grading homework and proctoring and grading exams.

Facebook, Inc. **Jun 19 - Sep 19**
Machine Learning Engineer Intern

- Built self-supervised sequence model in Caffe2 to train better user embedding from user history sequence and improve the click-through rate prediction of production ranking models.
- Improved the click-through rate prediction of several production ranking models by applying transfer learning between high-traffic channels and low-traffic channels.

NEC Laboratories America **Jun 18 - Dec 18**
Research Assistant, Department of Machine Learning

- Studied the problem of adversarial examples and propose optimal transport classifier (OT-Classifier), a novel unified end-to-end robust deep neural network framework against adversarial attacks, where the input image is first projected to a low-dimensional space and then classified.
- An objective was induced to minimize the optimal transport cost between the true class distribution and the framework output distribution, guiding the encoder and discriminator to project the input image to a low-dimensional space without losing important features.

- Extensive experiments demonstrated the robustness of our proposed OT-Classifier framework under the white-box attacks, and showed that OT-Classifier combined with adversarial training outperforms other state-of-the-art approaches on several benchmark image datasets.

SELECTED HONORS & AWARDS

- Peter Hall Graduate Research Award, 2020
- Graduation Honor Scholarship, 2014
- Shanghai Scholarship, 2013
- National Scholarship in China, 2011
- Freshman Scholarship, 2010

BOOK & CHAPTERS

1. **Yao Li**, Justin Wang, and Thomas CM Lee. Introduction to deep learning. *Wiley StatsRef: Statistics Reference Online (to appear)*, 2020

PUBLICATIONS

Google Scholar: `https://scholar.google.com/citations?hl=en&user=bQ6YhCwAAAAJ`

Refereed Conference Publications

1. Xuanqing Liu, **Yao Li**, Chongruo Wu, and Cho-Jui Hsieh. Adv-BNN: Improved adversarial defense through robust bayesian neural network. In *International Conference on Learning Representations*, 2019
2. Shuyi Liao, Angela Linderholm, Celeste Kivler, Lisa Franzi, Megan Showalter, **Yao Li**, Lihong Qi, Oliver Fiehn, Amir A Zeki, and Nicholas J. Kenyon. L-arginine intervention in severe asthma patients. *JCI Insight*, 5(13), 7 2020
3. **Yao Li**, Minhao Cheng, Kevin Fujii, Fushing Hsieh, and Cho-Jui Hsieh. Learning from group comparisons: Exploiting higher order interactions. In S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett, editors, *Advances in Neural Information Processing Systems 31*, pages 4981–4990. Curran Associates, Inc., 2018
4. Jinfeng Yi, Cho-Jui Hsieh, Kush R Varshney, Lijun Zhang, and **Yao Li**. Scalable demand-aware recommendation. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, *Advances in Neural Information Processing Systems 30*, pages 2412–2421. Curran Associates, Inc., 2017

Journal Publications

1. Qi Gao, Randy CS Lai, Thomas CM Lee, and **Yao Li**. Uncertainty quantification for high dimensional sparse nonparametric additive models. *Technometrics*, pages 1–12, 2019

Other Publications

1. **Yao Li**, Minhao Cheng, Thomas CM Lee, and Cho-Jui Hsieh. Adversarial examples: Attack and defense. *Journal of the American Statistical Association (to be submitted)*, 2020
2. **Yao Li**, Wenchao Yu, Martin Renqiang Min, Thomas Lee, Erik Kruus, Wei Wang, and Cho-Jui Hsieh. Detecting adversarial examples with regularized deep embedding. *Journal of Machine Learning Research (to be submitted)*, 2020
3. **Yao Li**, Martin Renqiang Min, Wenchao Yu, Cho-Jui Hsieh, Thomas Lee, and Erik Kruus. Improving the robustness of deep neural networks via embedding regularization. *Submitted to International Conference on Machine Learning*, 2020

TEACHING

At the University of California, Davis
Graduate level

- Optimization for Big Data Analytics, STA209, 2019 Fall, Teaching Assistant, 42 students
- Practice in Data Science, STA160, 2019 Spring, Teaching Assistant, 39 students

Undergraduate level

- Applied Statistics, STA103, 2017 Fall, Teaching Assistant, 62 students
- Elementary Statistics, STA13, 2018 Winter, Teaching Assistant, 50 students

GRANTS

PROFESSIONAL ACTIVITIES

Paper Reviewer

- Thirty-seventh International Conference on Machine Learning, 2020
- Thirty-Fourth AAAI Conference on Artificial Intelligence, 2020
- Neural Information Processing Systems, 2019
- Thirty-sixth International Conference on Machine Learning, 2019

Talks and Presentations

1. "Defending Against Adversarial Attacks by Regularized Deep Embedding", Presentation, Symposium on Data Science & Statistics, May, 2019
2. "Improved adversarial defense through robust bayesian neural network", Poster Presentation, International Conference on Learning Representations, May, 2019
3. "Learning from group comparisons: Exploiting higher order interactions", Poster Presentation, Neural Information Processing Systems, Dec, 2018
4. "Scalable demand-aware recommendation", Poster Presentation, Neural Information Processing Systems, Dec, 2017

RESEARCH INTERESTS

My main research focus is about improving the robustness of deep neural networks against adversarial examples. Previously, I have worked on recommendation systems, matrix factorization, crossover trials and additive models. Currently, I am interested in the problem of security for machine learning (adversarial deep learning).