

RUNTIAN ZHAI

zhairuntian@hotmail.com \diamond (+86) 189-6485-1630

www.runtianzhai.com \diamond Github: RuntianZ

EDUCATION

School of Electronics Engineering and Computer Science, Peking University (PKU)

B.S. in Computer Science (honors)

Sep 2016 - Jul 2020

- Major GPA: 3.75/4.0
- Research funded by MOE Top-notch Undergraduate Program. (20/350 students a year)
- Core courses: Data Structure and Algorithm (3.91), Algorithm Design and Analysis (3.92), Numerical Methods (3.85), Database Systems (3.81), Combinatorial Mathematics (3.99).
- Developed solid expertise in machine learning theory and applications. Over 200k lines of code in Python, Matlab, C/C++, Java, and PHP. Over 50k lines of code in PyTorch, Tensorflow and Keras.

School of Mathematical Sciences, PKU

B.S. in Applied Mathematics (Double Major)

Sep 2017 - Jul 2020

- Major GPA: 3.57/4.0
- Core courses: Mathematical Analysis (3.85), ODE (3.96), Complex Analysis (3.88), Probability Theory (3.77), Statistics (3.73), Math Modelling (3.97), Abstract Algebra (3.81).
- Developed solid skills in mathematical analysis, probability and statistics, and algebra.

School of Computer Science (SCS), Carnegie Mellon University (CMU)

Ph.D. in Machine Learning, Computer Science Department (CSD)

Aug 2020 -

- Will take online courses and do remote research starting from Aug 2020.

RESEARCH INTERESTS

Machine Learning Theory	Generalization, optimization, adversarial robustness
ML Algorithms	Semi-supervised/Unsupervised learning, transfer learning
ML Systems	Scalability, security, privacy

RESEARCH EXPERIENCE

Deep Learning Theory and Algorithms

Research Assistant. Advisor: Professor Liwei Wang, PKU

Jul 2018 - Present

- Studied adversarial training in the semi-supervised setting; Proved that more unlabeled data alone is able to improve adversarially robust generalization in the Gaussian mixture model.
- Proposed a robust training algorithm that learns with unlabeled data. Demonstrated through experiments that using unlabeled data achieves 10% higher accuracy than using labeled data alone.

Machine Learning Security

Research Assistant. Advisor: Professor Cho-Jui Hsieh, UCLA

Feb 2019 - Sep 2019

- Proposed MACER, an attack-free and scalable provable adversarial defense that trains l_2 -robust models by MAXimizing CERTified Radius.
- Empirically showed that MACER is better than state-of-the-art adversarial training in performance and runs much faster; Provided an extensive ablation study examining the effect of hyperparameters.

Deep Learning Application

Research Intern. Mentor: Di He, Microsoft Research Asia (MSRA) ML group

Sep 2019 - Jun 2020

- Proposed Transferred Discrepancy (TD), a new metric to measure the difference between the representations learned by two neural networks.
- Used TD to investigate the effect of various deep learning factors, and discovered that factors that improve deep learning always lead to more similar representations.

PUBLICATIONS AND MANUSCRIPTS

Y. Feng*, **R. Zhai***, D. He, L. Wang, B. Dong. Transferred Discrepancy: Quantifying the Difference Between Representations. arXiv: 2007.12446.

R. Zhai*, C. Dan*, D. He*, H. Zhang, L. Wang, P. Ravikumar, B. Gong, C.J. Hsieh. *MACER: Attack-free and Scalable Robust Training via Maximizing Certified Radius*. ICLR 2020.

R. Zhai*, T. Cai*, D. He*, C. Dan, K. He, J.E. Hopcroft, L. Wang. *Adversarially Robust Generalization Just Requires More Unlabeled Data*. arXiv: 1906.00555.

HONORS AND AWARDS

- Outstanding Undergraduate Researcher (top 5%) *Sep 2019*
- Research funded by MOE Top-Notch Undergraduate Program (20 students a year) *May 2019*
- Academic Excellence Award (top 5%) *Sep 2018*
- Meritorious Award for MCM/ICM (top 9%) *May 2018*
- Changfei Scholarship for Outstanding Students at PKU (top 5%) *Sep 2017*

STANDARDIZED TESTS

- GRE: 333 (Verbal: 163 (93%), Quantitative: 170 (96%)) Writing: 4.5 (81%)
- TOEFL: 113 (Reading: 30, Listening: 30, Speaking: 23, Writing: 30)