DINGHUAI ZHANG

(+86)18801216358 ⋄ zhangdinghuai@pku.edu.cn

EDUCATION

Peking University, Beijing *Sept. 2016 - Present*
Bachelor in Mathematics, School of Mathematical Sciences
Member of the Elite Undergraduate Training Program of Applied Math
GPA: 3.71/4.00 Rank: 1/13

RESEARCH INTERESTS

Bayesian methods, generative models, optimization, adversarial examples, probabilistic inference, optimal control

WORK EXPERIENCE

Undergraduate Research Assistant *May 2018 - Present*
Beijing Institute of Big Data Research
Deep Learning Lab of Peking University
Advisdor: Prof. Zhanxing Zhu

Visiting Research Assistant *July 2019 - Sept. 2019*
UT Statistical Learning & AI Group, University of Texas at Austin
Advisdor: Prof. Qiang Liu

PUBLICATION

Filling the Soap Bubbles: Efficient Black-Box Adversarial Certification with Non-Gaussian Smoothing. **Dinghuai Zhang***, Mao Ye*, Chengyue Gong*, Zhanxing Zhu, Qiang Liu *submitted to ICLR2020* OpenReview link (*Equal contribution)

You Only Propagate Once: Accelerating Adversarial Training via Maximal Principle. **Dinghuai Zhang***, Tianyuan Zhang*, Yiping Lu*, Zhanxing Zhu, Bin Dong *accepted by NeurIPS2019 and ICML2019 Security and Privacy of ML Workshop, arXiv preprint:1905.00877* (*Equal contribution)

Bridging Adversarial Robustness and Semi/Self/Un-supervised Learning. **Dinghuai Zhang** *accepted by NeurIPS 2019 Queer in AI Workshop*

RESEARCH EXPERIENCE

Adversarial Certification as Functional Optimization

Joint work with Chengyue Gong, Mao Ye, Zhanxing Zhu, Qiang Liu

- Propose a general framework of adversarial certification with non-Gaussian noise and for more general types of attacks, from a unified functional optimization perspective
- Identify a key trade-off between accuracy and robustness, helping to design two new families of non-Gaussian smoothing distributions that work more efficiently for ℓ_2 and ℓ_∞ attacks
- Achieve better results than previous works and provide a new perspective on randomized smoothing certification

Optimal Control View of Adversarial Training

Joint work with Tianyuan Zhang, Yiping Lu, Zhanxing Zhu, Bin Dong

- From an optimal control view, we reformulate adversarial training as a differential game and propose an accelerated algorithm YOPO (You Only Propagate Once) based on Pontryagin's Maximum Principle
- Gradient based YOPO can also be viewed as a splitting method for PGD adversarial training
- Achieve at least $4 \sim 5$ times faster speed

Semi-Supervised Learning via Sub-Manifold Regularization
Joint work with Bing Yu, Jingfeng Wu, Zhanxing Zhu

- Design a tangent regularization term and a normal regularization term along the manifold under manifold assumption
- Consider the manifold to be composed of many clusters of sub manifolds and design regularization for each manifold to punish the entanglement between different clusters of sub manifolds

Solving PDEs with Improved Deep Ritz Method
Joint work with Zeyu Jia, Zhengming Zou, supervised by Zhihua Zhang

- consider the manifold to be composed of many clusters of sub manifolds and design regularization for each manifold to punish the entanglement between different clusters of sub manifolds
- Build a neural network to minimize that parametrized functional
- Improve deep ritz method with self-adaptive sampling and actor critic sampling when computing the Monte Carlo integration of the functiona

MISC.

- Reviewer for ICLR2020
- Fangzheng Scholarship of Peking University
  Arawana Scholarship of Peking University
  Merit Student of Peking University (Top 5% in Peking University)
  Academic Innovation Award of Peking University

OTHER STRENGTHS

Computer Skills	Python, MATLAB, R and C LaTeX and Markdown
Standard Tests	GRE Math sub 910, 97% GRE Verbal 158, Quantitative 170, Analytical Writing 3.5 TOEFL 108 (Speaking 23)

PERSONAL HOBBIES

- Landscape & Street Photography : I am a huge fan of Daido Moriyama, a great Japanese photographer; I also crazily admire Henri Cartier-Bresson, father of modern documentary photograhphy
- Chinese Calligraphy : I reach level-9 which is the highest level for the non-professional artists