Feisi Fu

8 Saint Mary St, Photonics Center – Boston, MA, 02215

feisiwantjob@gmail.com Homepage
857-869-0444 LinkedIn/feisifu

SUMMARY

- A passionate **Machine Learning Ph.D. candidate** with a solid background in **Mathematics and Statistics**, strong proficiency in **Python**, experience in **open source project development**, and publications at **top-tier Machine Learning conferences (e.g., ICLR and NeurIPS).**
- 4 years of research experience in machine learning: 1. Familiar with **data preprocessing techniques (Sklearn)**; 2. Build state-of-the-art neural network models with **PyTorch** and **Tensorflow** (e.g., ResNet, RoBerta and ViT); 3. Train machine learning models in a cloud computing environment, like AWS. 4. **Edit neural network structure** to improve the performance, reduce the memory usage, or boost the training efficiency. 5. Visualize results with **Matplotlib**.

SKILLS

- Areas of Study: **Machine Learning, Machine Learning Safety, Neural Network Quantization**
- Related Courses: **Statistics, Dynamic Programming, Convex Optimization**
- Coding: **Python, PyTorch, Tensorflow, C++, CUDA C++**

EXPERIENCE

- **Research Scientist Intern at Meta, PyTorch Architecture Optimization Team** **Mentor: Zafar Takhirov**
  I leaded the project "Usage of Quantization in Neural Network Training". We have created the infrastructure for quantizing activation maps and conducted experiments on neural network training for ResNet50 on ImageNet (as a representative of convolutional neural networks) and RoBerta-large on GLUE (as a representative of NLP transformers). The experiments verified our analysis on memory saving and showed that by quantizing activation maps, we can save up to 50% of the training memory usage while sacrificing only 0.1% accuracy. *Aug. 2022 – Dec. 2022*
- **Graduate Teaching Fellow for Optimization Theory and Methods at Boston University**
  Sep. 2019 – Sep. 2021

EDUCATION

Boston University **Advisor: Prof. Wenchao Li**
Doctorate degree in Systems Engineering, GPA: 4.0/4.0 *2018 – 2023 (expected)*

Chinese Academy of Sciences, China **Advisor: Prof. Baohua Fu**
Master degree in Mathematics, GPA: 84.5/100 *2014 – 2018*

Sichuan University, China
Bachelor degree in Applied Mathematics, GPA: 89.2/100 *2010 – 2014*

PAPERS

- **Sound and Complete Neural Network Repair with Minimality and Locality Guarantees**[PDF]
  Feisi Fu, Wenchao Li
  Accept as a poster paper at International Conference on Learning Representations (ICLR), 2022

We present the first neural network repair methodology which applies only a localized change in the function space while guaranteeing the removal of buggy behavior.
Experiment Performance: 1. Repair Rate 96% (ReTrain) $\rightarrow$ guarantee 100% (ours); 2. Negative Side Effect 22.11% (Fine-Tuning) $\rightarrow$ 0.12% (ours).

- **REGLO: Provable Neural Network Repair for Global Robustness Properties**[PDF]
  Feisi Fu, Zhilu Wang, Jiameng Fan, Yixuan Wang, Chao Huang, Xin Chen, Zhu Qi, Wenchao Li
  Accept as a workshop paper at Neural Information Processing Systems (NeurIPS), 2022
  We present REGLO, the first work that enables provable repair of a neural network for global robustness properties.
  Experiment Performance: REGLO makes a neural network on German Credit dataset **global robust with less than 1% accuracy drop** (PGD-Bound $1.31 \rightarrow 0.028$ and Verification-Bound $12.5 \rightarrow 0.29$).
- **Dormant Neural Trojans**[PDF]
  Feisi Fu, Panagiota Kiourti, Wenchao Li
  We present a novel methodology for neural network backdoor attacks, inserting a Trojan that will remain dormant until activated. The dormant Trojan can bypass the most state-of-the-art backdoor detention methods.
- **OVLA: Neural Network Ownership Verification using Latent Watermarks**
  Feisi Fu, Wenchao Li
  We present a novel methodology for neural network ownership verification by decoupling a network's normal operation from its responses to watermarked inputs during ownership verification.
  Experiment Performance: Add a watermark to a DNN for ownership verification with **less than 1% accuracy drop**.
- **A Tool for Neural Network Global Robustness Certification and Training**[PDF]
  Zhilu Wang, Yixuan Wang, Feisi Fu, Ruochen Jiao, Chao Huang, Wenchao Li, Qi Zhu
  We propose a GPU-supported global robustness certification framework GROCET which is more efficient than any previous optimization-based certification approaches.
- **A Study of Complement Problem for Plane Curves**
  Feisi Fu, Baohua Fu
  We will describe the isomorphisms between complements of irreducible closed curves in the complex affine plane C^2, which do not extend to an automorphism of C^2.

COMPETITIONS

- **TrojAI Competition by National Institute of Standards and Technology**
  Feisi Fu, Jiameng Fan, Weichao Zhou, Panagiota Kiourti, Sabbir Ahmad, Wenchao Li
  We train a neural network to analyze the eigenvalues of a given network's weights and detect if such network has a Trojan. Our approach achieves the top 5 ROC-AUC among all approaches.

REVIEWER FOR JOURNALS & CONFERENCE ARTICLES

- **AAAI Conference on Artificial Intelligence (AAAI), 2023**
- **Workshop on Trustworthy and Socially Responsible Machine Learning, NeurIPS, 2022**
- **Design Automation Conference (DAC), 2020, 2022**
- **Design Automation and Test in Europe (DATE), 2021, 2022**
- **International Conference on Dependable Systems and Networks (DSN), 2021, 2022**
- **Hybrid Systems: Computation and Control (HSCC), 2020**
- **International Conference on Computer-Aided Design (ICCAD), 2021**
- **International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2020**