Qiuling Xu

765-701-5968 | xu1230@purdue.edu | QiulingXu.github.io | Google Scholar

Education

Purdue University Major GPA: 3.67/4
PhD in Computer Science, West Lafayette, Indiana, USA *Aug. 2018 – May 2023 (expected)*

Nanjing University Major GPA: 4.37/5
BS in Computer Science, Nanjing, Jiangsu, China *Aug. 2014 – May 2018*

Experience

Research Intern *Mar. 2018 – June 2018*
Microsoft Research *Beijing, China*

- Designed hyper-parameter searching space representation for ***user-friendly Automatic Machine Learning***.
- Improved the internal tools (public at github.com/microsoft/nni).

Research Assistant *Aug. 2018 – Present*
Purdue University *West Lafayette, IN*

- Improved attack successful rate ***60%***+ on adversarially trained models by Feature Space Attack.
- Created adversarial samples ***20%***+ more imperceptible under the same threat level by Deep Distribution Bound.
- Provided general information-theoretic robustness upper bound for regression, classification and estimation tasks.
- Explored methods for defense, explanation and analysis of adversarial attack in ***Adversarial Learning***.

Research Assistant *Aug. 2016 – June 2018*
Nanjing University *Nanjing, China*

- Devised an end-to-end module to learn logical reasoning and neural perception simultaneously.
- Improved ***80%*** accuracy over baselines including ***DeepMind's DNC***.
- Explored variance reduction for ***policy gradient*** algorithm in robust ***Reinforcement Learning***.

Awards

Top 1% in ACM-ICPC International Programming Contest China ***Final*** (16/1500) *2016, Shanghai, China*

Publications (* represents equal contribution)

Bridging Machine Learning and Logical Reasoning by Abductive Learning
WangZhou Dai, **Qiuling Xu***, Yang Yu* and Zhihua Zhou* **NeurIPS 2019**

Trace Divergence Analysis and Embedding Regulation for Debugging Recurrent Neural Networks
*Guanhong Tao, Shiqing Ma, Yingqi Liu, **Qiuling Xu** and Xiangyu Zhang* **ICSE 2020**

Deep Distribution Bound for Nature-looking Adversarial Attack
***Qiuling Xu**, Guanhong Tao and Xiangyu Zhang* Preprint

Towards Feature Space Adversarial Attack
***Qiuling Xu**, Guanhong Tao, Siyuan Cheng and Xiangyu Zhang* Preprint

Fundamental Limits of Adversarial Learning
Qiuling Xu, Kevin Bello* and Jean Honorio* Preprint

Projects

Gender-fair Word Embedding | *Python, NLP, Adversarial Learning* *June 2020*

- Enforced word embedding's fairness by Adversarial Training; decreased 20%+ more correlation than the SOTA.

Operating System | *C, Assembly Language, Operating System* *June 2016*

- Implemented OS from scratch, including boot, system call, driver, memory, file, process, and shell.

Sub C Compiler | *C, Bison, Lex* *June 2017*

- Implemented term extraction, syntax & semantic analysis, and grammar tree & intermediate code translation.

Technical Skills

Courses: NLP, Machine Learning(ML) Theory, Reinforcement Learning, Graph ML, Statistical ML
Languages: Python, C/C++ **Frameworks**: Tensorflow, Pytorch, MXNET **Libraries**: NumPy, Matplotlib