Tianqi Chen

tqch@utexas.edu 1 (734) 882-3951 tqch.github.io

Education

University of Texas at Austin Austin, TX
PhD in Statistics — Aug. 2021 – (estimated) May 2026

University of Michigan Ann Arbor, MI
Master of Science in Applied Statistics — Sept. 2019 – Apr. 2021

Fudan University Shanghai, China
Bachelor of Science in Mathematics and Applied Mathematics — Sept. 2015 – June 2019

Publications and preprints

ASK: Adversarial Soft k-Nearest Neighbor Attack and Defense June 2021
preprint
https://arxiv.org/pdf/2106.14300.pdf

- We proposed a novel information-theoretic loss function as a differentiable surrogate of kNN classification error, based on which we developed a new attack method, ASK-Attack, that outperforms existing kNN attacks by a large margin.
- We further devised ASK Defense, a regularized adversarial training strategy built upon ASK loss. To best of our knowledge, it is the first algorithm that effectively defends against kNN attacks on hidden layers of DNNs.
- We conducted extensive experiments on hyperparameter sensitivity as well as provided detailed ablation study on all the components used in both ASK Attack and ASK Defense.

Immuno-mimetic Deep Neural Networks (Immuno-Net) June 2021
The 2021 ICML Workshop on Computational Biology
https://arxiv.org/pdf/2107.02842.pdf

- We proposed a general biomimetic evolutionary algorithm intended for robustification of deep neural networks (DNNs).
- The algorithm can further improve the classification performance of state-of-the-art methods on typical machine learning datasets such as SVHN & CIFAR10 under adversarial setting.

RAILS: A Robust Adversarial Immune-inspired Learning System Dec. 2020
IEEE Access
https://ieeexplore.ieee.org/document/9718107

- We proposed a novel adversarial learning framework inspired by mammalian immune system, which is agnostic to backbone neural network architectures and adaptive to unseen attacks.
- We also empirically showed that RAILS can improve the robustness of DNN classifiers with different model structures (e.g., VGG16 and ResNet18) and various SOTA adversarial attacks (e.g., CW, PGD, Square and HopSkipJump).

Projects

GARD: Guaranteeing AI Robustness Against Deception July 2020 – July 2021
Research Assistant

- Studied the mechanism of mammalian immune system and adapted the antibody generation process to a novel adversarial learning defense strategy.
- Facilitated the program evaluation phase II/III as a member of team UMich.

UM-OIG Project: High-dose Opioid Transaction Prediction and U.S. Medicaid Pharmacy Fraudulence Risk Evaluation May 2020 – Sept. 2020
Student Statistician

- Processed ~500M transaction data from the Michigan Department of Health and Human Service, derived predictor variables including morphine milligram equivalents and opioid-involved overdose death rate by CDC prescription guideline and Michigan demographic data.
- Investigated the relationship between high-dose opioid transaction with factors such as pharmacy ownership, geographical location, and patient composition with weighted least square linear models.
- Built three models using standard logistic regression, random forest, and non-ignorable missing data methods (Ibrahim and Lipschitz algorithm with Firth penalty) and compared the model performances on the holdout set.

Jobs

Department of Information, Risk, and Operations Management, University of Texas at Austin June 2021 - Present
Teaching Assistant

Student Technician

Department of Statistics, University of Michigan May 2020 – Apr. 2021
Graduate Student Instructor
Course Grader

Skills

Programming: proficient in Python, R and SQL
Data Science & Machine Learning: familiar with NumPy, pandas, scikit-learn; experienced in TensorFlow and PyTorch
Language: Chinese (native), English (advanced), Japanese (intermediate)

Fellowships and Awards

UT Austin Graduate School Recruitment Fellowship July 2021
3rd Prize, Shanghai College Student Mathematics Competition Oct. 2016
1st Prize, Fudan University Excellent Freshman Scholarship Oct. 2015