Calvin **Xu**

Champaign, IL | cx23@illinois.edu | 978.427.9392
github://cmxu | cmxu.io | stack://cmxu

Research Interests

I am a PhD Student in the Department of Computer Science at the University of Illinois Urbana-Champaign (UIUC). My research interests lie in ***robust*** and ***formally verifiable*** machine learning. Specifically, I am currently focused on exploring adversarial examples and leveraging them to understand the behavior of deep learning systems. I am also interested in robust generation of adversarial examples, neural network repair, neural network verification, and the intersection of explainable and robust ML.

Education

Current
Sep 2021

PhD Student at University of Illinois at Urbana-Champaign
Working on **PhD** in **CS**, GPA: 4.0/4.0

Dec 2019
Aug 2019

Advanced Studies Student at Massachusetts Institute of Technology
Coursework - Advances in Computer Vision (6.869), GPA: 5.0/5.0

Dec 2018
Aug 2018

Graduate Student at Washington University in St. Louis
MS in **CS**, Certificate in Data Mining & Machine Learning, GPA: 3.9/4.0

May 2018
Aug 2015

Undergraduate Student at Washington University in St. Louis
BS in **Mathematics** and **BS** in **CS**, GPA: 3.9/4.0

Research/Teaching Experience

Current
Aug 2021

PhD Student at University of Illinois in Urbana-Champaign
Currently researching Universal Adversarial Perturbations (UAPs). Developed technique for generating Robust UAPs which have strong potential for creating real-world attacks. Work in submission at ***ICML 2022***. Created and implemented technique for unsupervised UAP generation. Working on verification techniques for wireless systems.

Dec 2018
Sep 2016

Teaching Assistant at Washington University in St. Louis
Graded and held office hours for graduate level Machine Learning (150 students) and Numerical Applied Mathematics (50 students). Designed, ran, and graded the final project for the Machine Learning course.

Mar 2018
Jun 2017

Research Assistant at Carnegie Mellon University
Employed Adversarial ML techniques to thwart Android Malware detection and other defect prediction algorithms. Developed theory for attacking and defending high dimensional Support Vector Machines. Implemented data poisoning attacks on the Drebin Android Malware dataset, and presented poster at CMU. Proved that ~10 poisoned data points can be enough to significantly reduce the effectiveness of the malware detector.

May 2017
Jun 2016

Research Assistant at Washington University in St. Louis
Created benchmarks and proved correctness for a work-stealing scheduler, improving cache efficiency by factor of 2. Rigorously proved a nearly series parallel race detection algorithm which matched asymptotic runtime of series parallel case. Co-authored ***Race Detection and Reachability in Nearly Series-Parallel DAGs***, published in ***ACM-SIAM SODA***.

Work Experience

May 2021
Mar 2019

Associate Staff at **MIT Lincoln Laboratory** (Top Secret Clearance)
Applied DAGAN to network traffic to augment unbalanced classes resulting in a ~20% increase in classification accuracy. Applied CNNs, Word2Vec, and Q-Learning techniques to flight data to predict flight reroutes, published at ***INFORMS***. Gathered dataset and built system using NLP and Neural Networks (NNs) to determine when to apply Adversarial ML. Explored Semantic Adversarial Examples and Spatial Transformer Networks for data augmentation. Developed an algorithm using GANs and Non-Negative NNs that won 1st place at AdvML Challenge at ***SigKDD 2019***.

Aug 2018
May 2018

Intern at **EUB-INC** in Beijing, China
Leveraged neural networks and clustering to automate user grouping for data-driven advertisement on WeChat. Developed algorithm which reduced turnaround time by 90% for data team, allowing for faster, more targeted advertisement.

Awards

Apr 2018	Dean’s Select Fellowship for Research Excellence (WUSTL)
Dec 2015-17	Putnam Exam: 28, 20, 12
Aug 2015	Compton Scholar for Mathematics and Physics (4 per grade)
Apr 2017	Missouri Math Competition: 1st Place Team
Dec 2015	ICPC Regional: Top 5 Team

Skills

Languages	English (Native), Chinese (Fluent), Japanese (Basic Knowledge)
ML Libraries	Tensorflow, Torch, Keras, Theano, Weka, Scikit-Learn, Spark
Coding	Python, Java, Matlab, R, Javascript, C, C++, Android, Mathematica

Coursework

Math Differential Equations, Matrix Algebra, Calculus of Several Variables, Introduction to Analysis, Number Theory and Cryptography, Numerical Applied Mathematics, Introduction to Lebesgue Integration, Topics in Applied Mathematics: Mathematics for Multimedia, Linear Algebra, Probability, Bayesian Statistics, Mathematical Statistics, Time Series Analysis, Statistical Computation

CS Programming Skills Workshop, Algorithms and Data Structures, ***Machine Learning***, Object Oriented Software Development Laboratory, Introduction to System Software, ***Introduction to Artificial Intelligence***, ***Computational Geometry***, ***Data Mining***, ***Multi-Agent Systems***, ***Topological Applications for Data Analysis and Machine Learning***, ***Approximation Algorithms***, ***Algorithms for Nonlinear Optimization***, ***Sparse Modeling for Imaging and Vision***, ***Systems Security***, ***Algorithms for Computational Biology***, ***Advanced Topics in Computer Vision***†, ***Statistical Reinforcement Learning***’, ***Logic and AI***’, ***Adv Topics in Sec, Priv and ML***’
Graduate Level, † MIT, ’ UIUC