Sterling Suggs

Reliable and friendly ML researcher/engineer with a math foundation and 5+ years of experience in computer vision, reinforcement learning, and adversarial ML.

sterlingwsuggs@gmail.com swsuggs.github.io/ github.com/swsuggs linkedin.com/in/swsuggs

Experience

Senior ML Research Scientist | *Two Six Technologies* July 2021 – Present

- Develop and maintain Armory, an open source framework for evaluating ML defenses against adversarial attacks. Create and integrate new datasets, metrics, attacks, defenses, visualizations, and other tools
- Plan and execute bi-annual ML evaluation cycles (defense and attack) for the DARPA GARD program, coordinating teams at over a dozen participating institutions
- Analyze defended and undefended ML models for vulnerabilities and biases
- Serve as primary POC for 100+ Armory users, providing technical support and transforming feedback into new features and measurable improvements
- Mentor and direct junior team members and new hires
- Paper: Benchmarking the Effect of Poisoning Defenses on the Security and Bias of Deep Learning Models

Research Assistant | *BYU Computer Science Dept.* 2017 – 2021

- Designed and implemented several read/write memory-augmented DNNs, increasing effective memory size 16X
- Incorporated attention-based auxiliary memory into deep reinforcement learning and studied the effect on sample efficiency, representation learning, and meta-learning
- Investigated capability of RL agents to transfer across data distributions and learn faster than pure gradient propagation

Software Engineer | *Veracity Forecasting and Analysis* 2016 – 2017

- Simulated the recruitment and supply chain for a large US defense department, pinpointing bottlenecks and potential optimization points
- Programmed physics-based model of solid rocket motor fuel to improve prediction of failure probability over time
- Automated data collection for human resource planning, saving hours of weekly manual effort

Developer | *BYU Mathematics Dept.* 2015 – 2016

- Drafted and refined new scientific computing and data science programming labs for university curriculum (example: Generalized Minimal Residuals)
- Wrote new course material to teach math majors Python programming (example: Graphical User Interfaces)

Education

M.S. Computer Science | *Brigham Young University* 2021

- Machine Learning emphasis
- Thesis: Reinforcement Learning with Memory Networks
- GPA: 3.93/4.0

B.S. Applied Mathematics | *Brigham Young University* 2017

- Computer Science minor
- GPA: 3.91/4.0

Technical Competencies

Skills: Deep Neural Networks, Computer Vision, Reinforcement Learning, Adversarial ML, AI safety, Natural Language Processing, Bayesian Statistics, Multi-agent systems, Algorithm Design and Optimization, Control Theory, ODE/PDEs, Mathematical Analysis

Tools: Python, C++, Java, Pytorch, Tensorflow, Pandas, Scipy, Scikit-learn, Docker, MongoDB, LaTex, Unix shell, Slurm, Git, Mercurial, AWS, Bash, HMTL, CSS, SQL