Xuanqing Liu

September 28, 2019
xqliu@cs.ucla.edu
(+1) (530)601-8272

Education

- **University of California, Los Angeles** — Los Angeles, CA
  Ph.D. student in computer science. Advisor: Cho-Jui Hsieh — *2018-*
- **University of California, Davis** — Davis, CA
  Ph.D. student in computer science. Advisor: Cho-Jui Hsieh — *2016 - 2018*
- **Peking University** — Beijing, China
  B.Sc in physics. Advisor: Qite Li and Yansong Feng — *2011 - 2016*
  †Thesis: Simulation and Optimization of Cosmic Ray Muon Imaging Detector

Research interests

Optimization: Convex and non-convex optimization for models in machine learning.

- Extending inexact subsampled Newton-type method to support non-smooth regularizers.
- Variance reduction SGD with random batch size, cache-aware SAGA.
- Efficient solver for Trust-region subproblem.

Security issues of deep neural networks: threats and defense methods.

- Neural networks that are robust to adversarial attacks.
- Adversarial neural networks.

Publication & preprints

- Lu Wang, **Xuanqing Liu**, Jinfeng Yi, Zhi-Hua Zhou, Cho-Jui Hsieh. *Evaluating the Robustness of Nearest Neighbor Classifiers: A Primal-Dual Perspective.* ArXiv preprint (2019).
- **Xuanqing Liu**, Tesi Xiao, Si Si, Qin Cao, Sanjiv Kumar, Cho-Jui Hsieh. *Neural SDE: Stabilizing Neural ODE Networks with Stochastic Noise.* ArXiv preprint (2019).
- **Xuanqing Liu**, Cho-Jui Hsieh, Jason D. Lee, Yuekai Sun. *An Inexact Subsampled Proximal Newton-type Method for Large-scale Machine Learning.* ArXiv preprint.
- **Xuanqing Liu**, Jason D. Lee, Cho-Jui Hsieh. *Better Generalization by Efficient Trust-region Method.* Draft.

- **Xuanqing Liu**, Si Si, Xiaojin(Jerry) Zhu, Yang Li, Cho-Jui Hsieh. *A Unified Framework for Data Poisoning Attack to Graph-based Semi-supervised Learning.* NeurIPS 2019.
- Wei-Lin Chiang, **Xuanqing Liu**, Si Si, Yang Li, Samy Bengio, Cho-Jui Hsieh. *Cluster-GCN: An Efficient Algorithm for Training Deep and Large Graph Convolutional Networks.* KDD 2019.

- **Xuanqing Liu**, Cho-Jui Hsieh. *From Adversarial Training to Generative Adversarial Networks.* CVPR 2019.
- **Xuanqing Liu**, Yao Li*, Chongruo Wu*, Cho-Jui Hsieh. *Adv-BNN: Improved Adversarial Defense through Robust Bayesian Neural Network.* ICLR 2019.
- **Xuanqing Liu**, Minhao Cheng, Huan Zhang, Cho-Jui Hsieh. *Towards Robust Neural Networks via Random Self-ensemble.* ECCV 2018.
- **Xuanqing Liu**, Cho-Jui Hsieh. *Fast Variance Reduction Method with Stochastic Batch Size.* ICML 2018.

Industrial Experience

- Fall/Winter 2019. Amazon Inc. *Applied Research Intern*
  Topic: Machine translation.
- Fall/Winter 2018. Google Research. *Student Research Collaborator*
  Topics: Model compression, data poisoning, graph neural networks.
- Summer 2018. Criteo AI Research. *Research Intern*
  Topic: Gradient boosting neural networks for commercial ads prediction.

Academic Services

Reviewer for ICML, NeurIPS, CVPR, ICCV, IJCAI, AAAI and TPAMI.

Programming languages and tools

- **Programming Languages:** C/++, Python, etc.
- **Tools:** PyTorch, Theano.
- **GitHub:** https://github.com/xuanqing94.

Awards, grants & honours

ICLR student travel grant	2019
Graduate Scholars Fellowship at UC Davis	2016
The Okamatsu Scholarship at Peking University	2014