Sahil Singla

4120, Brenden Iribe Center
University of Maryland

Phone : +1.475.228.4315
Email : ssingla@cs.umd.edu
Web: singlasahil14.github.io/

Education

- **University of Maryland** — College Park, MD
  PhD thesis: Certifiably robust deep learning systems; GPA: 4.00 — *Aug. 2018 – Present*
- **Indian Institute of Technology, Delhi** — New Delhi, India
  Bachelor of Technology in Computer Science; GPA: 8.16/10.0 — *Aug. 2010 – July. 2014*

Publications

- **Sahil Singla**, Soheil Feizi. **Second-Order Provable Defenses against Adversarial Examples**. Accepted at **ICML, 2020**.
  https://arxiv.org/abs/2006.00731
- **Sahil Singla**, Eric Wallace, Shi Feng, Soheil Feizi. **Understanding Impacts of High-Order Loss Approximations and Group Features in Interpretation.** Accepted at **ICML, 2019**.
  https://arxiv.org/abs/1902.00407
- Alexander Levine, **Sahil Singla**, Soheil Feizi. **Certifiably Robust Interpretation in Deep Learning**. Under Review. Short version accepted at NeurIPS Workshop on Machine Learning with Guarantees, 2019.
  https://arxiv.org/abs/1905.12105
- **Sahil Singla**, Soheil Feizi. **Bounding Singular Values of Convolutional Layers.** Under review. Short version accepted at ICLR workshop on Trustworthy Machine Learning, 2020.
  https://arxiv.org/abs/1911.10258
- Cassidy Laidlaw, **Sahil Singla**, Soheil Feizi. **Perceptual Adversarial Robustness: Defense Against Unseen Threat Models** Under review.
  https://arxiv.org/abs/2006.12655
- Vedant Nanda, Samuel Dooley, **Sahil Singla**, Soheil Feizi, John Dickerson. **Fairness Through Robustness: Investigating Robustness Disparity in Deep Learning** Under review.
  https://arxiv.org/abs/2006.12621
- **Sahil Singla**, Soheil Feizi. **Robustness Certificates Against Adversarial Examples for ReLU Networks.** Preprint.
  https://arxiv.org/abs/1902.01235

Awards and Academic achievements

- **Dean's Fellowship**. Cash prize of $2500. Awarded to only two students in the first and second year in the Computer Science department at University of Maryland.
- Secured **All India Rank 47** out of half a million students (amongst top .01% of the students) who appeared in **IIT-JEE 2010** exam
- State Rank 3 and **All India Rank 56** out of one million students (amongst top .005% of the students) in **AIEEE-2010** exam

Research interests

Robustness certificates, Adversarial attacks, Interpretation of deep learning

Experience

- **Goldman Sachs** — Bangalore, India
  Analyst — *August 2014 - August 2015*
  - Worked on reducing the time taken for pricing options.
  - Developed a software to calculate various risks associated with options portfolio
- **WaltonPay** — New Delhi, India
  Cofounder and CTO — *August 2015 - March 2016*
  - Developed a mobile app that would gather SMS data for credit evaluation.
  - Designed a statistical model to evaluate a persons credit profile based on SMS data.
- **Farmguide** — Gurgaon, India
  Machine Learning Engineer — *April 2016 - March 2017*
  - Developed a software to segment farm boundaries from satellite imagery
  - Work was featured in Forbes and is currently being used by Government of India
- **APUS** — Gurgaon, India
  Machine Learning Engineer — *April 2017 - July 2017*
  - Implemented neural style transfer that runs faster than popular app Prisma on phone.
  - Implemented the tensorflow op for sparse convolution in C++ that can run on mobile phone.
- **Computer Vision Consulting** — Gurgaon, India
  Consultant — *August 2017 - December 2018*
  - Use satellite imagery to identify areas of low and high agriculture produce.
  - Use computer vision to estimate weight of agriculture produce in a container.
- **Quadeye Securities** — Gurgaon, India
  Quantitative Analyst — *Jan 2018 - August 2018*
  - Designed a machine learning model to predict whether to buy/sell based on analyst ratings.
  - Designed a statistical model to reduce the runtime of an algorithm for strategy optimization.

Open Source Projects

- Designed a new kind of pooling layer based on sorting and averaging that improves accuracy and speed of convergence over max pooling on several state-of-the-art benchmarks.
- Designed a new loss function to add to the standard cross entropy loss function for the problem of image classification. Showed improvements over several baselines and datasets and different architectures.
- A thorough analysis of how various hyperparameters of loss configuration affect the results of neural style-transfer.
- Analyzed how inception architectures could be tweaked and used as loss networks for style transfer. Documented how different hyperparameter configurations of the loss network affect results of style-transfer.
- Designed a new kind of convolution operation where the filters of convolution operation were orthogonal to one another. Matched the baseline results while keeping the filters orthogonal.

References

- Soheil Feizi
  - Assistant Professor, University of Maryland, College Park
  - Email: sfeizi@cs.umd.edu
  - Phone: (857) 600-8157
- David Jacobs

    - Professor, University of Maryland, College Park
    - Email: djacobs@cs.umd.edu
    - Phone: (301) 405-0679
- Abhishek Sharma
    - Staff Research Scientist, Facebook
    - Email: abhisharayiya@gmail.com
    - Phone: (240) 476-8060