Muni Sreenivas Pydi

Contact Information

Website: https://munisreenivas.github.io/ *E-mail:* pydi@wisc.edu

Research Interests

Trustworthy Machine Learning—adversarial robustness, differential privacy and fairness; Optimal Transport applications to Machine Learning, Learning on Graphs.

Education

University of Wisconsin-Madison, Madison, WI, USA
PhD in Electrical Engineering with Minor in Statistics 2019 - Present
Advisor: Prof. Varun Jog

Master of Science in Electrical Engineering 2017 - 2019
Advisors: Prof. Varun Jog and Prof. Po-Ling Loh

Indian Institute of Technology (IIT) Madras, Chennai, India
Bachelor of Technology (Honours) in Electrical Engineering 2010 - 2014

Publications

1. **The Many Faces of Adversarial Risk**
Muni Sreenivas Pydi and Varun Jog
Neural Information Processing Systems (NeurIPS), 2021.
2. **Adversarial Risk via Optimal Transport and Optimal Couplings**
Muni Sreenivas Pydi and Varun Jog
IEEE Transactions on Information Theory, 2021.
3. **Adversarial Risk via Optimal Transport and Optimal Couplings**
Muni Sreenivas Pydi and Varun Jog
International Conference on Machine Learning (ICML), 2020.
4. **Active Learning with Importance Sampling**
Muni Sreenivas Pydi and Vishnu Lokhande
NeurIPS Workshop on ML with Guarantees, 2019.
5. **Graph-Based Ascent Algorithms for Function Maximization**
Muni Sreenivas Pydi, *Varun Jog and Po-Ling Loh*
Allerton Conference on Communication, Control and Computing, 2018.
6. **On Consistency of Compressive Spectral Clustering**
Muni Sreenivas Pydi, *and Ambedkar Dukkipati*
IEEE International Symposium on Information Theory (ISIT), 2018.
7. **Random access retransmission scheme for power limited nodes**
Karthik Nagasubramanian, and **Muni Sreenivas Pydi**
IEEE National Conference on Communications (NCC) India, 2017.
8. **Analytic Connectivity of General Hypergraphs**
Ashwin Guha, **Muni Sreenivas Pydi**, *Biswajit Paria and Ambedkar Dukkipati*
arXiv preprint arXiv:1701.04548, 2017.

Research Experience

University of Cambridge, Cambridge, UK
Visiting Student (Statistical Laboratory) May 2022 - Present
- Research on developing practical algorithms based on submodular optimization for obtaining provably robust machine learning classifiers.

Nokia Bell Labs, New Providence, NJ, USA (Remote work)
Research Intern June 2021 - Aug 2021
- Developed a meta-learning algorithm for Model Agnostic Meta Learning (MAML) where task-specific gradient updates are matched using optimal transport theory.

University of Wisconsin-Madison, Madison, WI, USA
Research Assistant (Department of ECE) June 2019 - May 2021

- Research at the intersection of machine learning, statistics and information theory with the goal of understanding the fundamental limits of adversarial robustness in machine learning tasks.

Indian Institute of Science (IISc), Bengaluru, India
Research Assistant (Statistics and Machine Learning Lab) Aug 2016 - Jul 2017

- Proved the asymptotic consistency of a compressive spectral clustering algorithm over the stochastic block model for graph structured data. Research on hypergraph clustering.
- Developed deep learning models to classify underwater objects using passive sonar signals for a joint project with the Defence Research and Development Organisation (DRDO), India.

Teaching Experience

University of Wisconsin-Madison, Madison, WI, USA
Teaching Assistant (Department of ECE) Jan 2019 - May 2019

- TA for CS 532: Matrix Methods for Machine Learning — graduate-level class of size > 50, taught by Prof. Po-Ling Loh. Ran hands-on deep learning lectures, held review sessions.

Teaching Assistant (Department of Computer Science) Aug 2018 - Dec 2018

- Head TA for CS 761: Mathematical Foundations of Machine Learning — graduate-level class of size > 100, taught by Prof. Rob Nowak. Held review sessions, graded homeworks & quizzes.

Teaching Assistant (Department of Mathematics) Aug 2017 - May 2018

- TA for Math 240: Introduction to Discrete Mathematics
- TA for Math 171: Calculus with Algebra and Trigonometry I

Industrial Experience

Samsung R&D Institute, Bengaluru, India
Senior Software Engineer (4G/LTE protocol stack development) Aug 2014 - Jul 2016

- Formulated an improved random access scheme for wireless communication, that opportunistically schedules retransmissions for power limited nodes (IoT, sensor networks). Paper published at IEEE National Conference on Communications, India.
- Developed and maintained protocol stack for the largest 4G/LTE deployment project in India, in PHY/MAC layers. Designed and developed a Python based parsing tool from the ground up, to analyse the LTE eNodeB schedule logs. Received a Spot Award for the contribution.

Deutsche Bank, Mumbai, India
Summer Intern (Statistical Modeling) May 2013 - Jul 2013

- Developed stochastic models for life expectancy forecasting using time series methods including ARIMA and regression. Developed a longevity index option pricing model in R.

Indian Space Research Organization, Sriharikota, India
Summer Intern (Digital System Design) Jun 2012 - Jul 2012

- Programmed FPGA for antenna-pointing of the multi-object tracking radar at the Satish Dhavan Space Center.

Technical Skills

Programming: Python, MATLAB, C, Java, R
Machine Learning: PyTorch, Keras, scikit-learn

Graduate Coursework

Machine Learning (ML)/CS	**Statistics/Math/Control**
Theoretical ML	Robust Statistics
Foundations of ML	Information Theory
Advanced Learning Theory	Topics in Probability, Theory of Probability
Large Scale ML & Optimization	Linear Systems, Nonlinear systems
Optimal Transport for ML	Real Analysis, Analysis I-II
Advanced Algorithms	Optimiztion in Statistical Settings

Invited Talks

1. **Adversarial Robustness via Optimal Transport** June 2022
   Host: Prof. Po-Ling Loh
   Institute of Mathematical Statistics Annual Meeting, London, UK.
2. **Theoretical Foundations of Adversarial Robustness** Apr 2022
   Host: Prof. Shuchin Aeron
   Tufts ECE Graduate Seminar (online), Tufts University, USA.
3. **Theoretical Foundations of Adversarial Robustness** Jan 2022
   Host: Prof. Clement Royer
   MILES (Machine Intelligence & Learning Systems) Seminar (online), PSL-Dauphine, France.
4. **Introduction to Adversarial Learning** Feb 2021
   Host: Prof. Mangal Kothari
   Workshop on Decision & Control: Optimal Planning, ML & Games (online), IIT Kanpur, India.
5. **On Consistency of Compressive Spectral Clustering** Aug 2018
   Host: Prof. Robert Nowak
   Summer SILO (Systems, Information, Learning & Optimization) Seminar, UW-Madison, USA.

Service

Reviewer for IEEE International Symposium on Information Theory (ISIT), Asian Conference on Machine Learning (ACML), Information and Inference: A Journal of the IMA, International Conference on Algorithmic Learning Theory (ALT).

Honours and Achievements

IEEE International Symposium on Information Theory (ISIT) Student Travel Award, 2018.

Jury Award, Samsung R&D, for the best poster at the annual Samsung R&D Tech Fair, 2015.

Advanced-level Software Competency Certification at Samsung R&D. (10% of employees), 2015.

Spot Award, Samsung R&D, for outstanding contribution towards project, 2015.

Conferral of the Honours degree in EE, IIT Madras, 2014.

CBSE Merit Scholarship, Central Board of Secondary Education (CBSE) India, 2010-2014.

Ranked All India 243 out of 470,000 candidates in IIT Joint Entrance Exam, 2010.

Ranked All India 70 out of a million candidates in All India Engineering Entrance Exam, 2010.