Muni Sreenivas Pydi

Contact Information

Website — Linkedin — Google Scholar — Email

muni.pydi@lamsade.dauphine.fr; munisreenivas@gmail.com.

Research Interests

Trustworthy Machine Learning— robustness, privacy and fairness; Optimal Transport applications to Machine Learning, Generative Models.

Education

University of Wisconsin-Madison, Madison, WI, USA

PhD in Electrical Engineering with Minor in Statistics 2019 - 2022

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. **Unveiling the Role of Randomization in Multiclass Adversarial Classification: Insights from Graph Theory**
   Lucas Gnecco Heredia, Matteo Sammut, **Muni Sreenivas Pydi**, Rafaël Pinot, Benjamin Negrevergne and Yann Chevaleyre
   International Conference on Artificial Intelligence and Statistics (AIStats), 2025.
2. **Optimal Classification under Performative Distribution Shift**
   Edwige Cyffers, **Muni Sreenivas Pydi**, Jamal Atif, Olivier Cappé
   Neural Information Processing Systems (NeurIPS), 2024.
3. **Optimal Budgeted Rejected Sampling for Generative Models**
   Alexandre Verine, **Muni Sreenivas Pydi**, Benjamin Negrevergne and Yann Chevaleyre
   International Conference on Artificial Intelligence and Statistics (AIStats), 2024.
4. **On the Role of Randomization in Adversarially Robust Classification**
   Lucas Gnecco Heredia, **Muni Sreenivas Pydi**, Benjamin Negrevergne and Yann Chevaleyre
   Neural Information Processing Systems (NeurIPS), 2023.
5. **Precision-Recall Divergence Optimization for Generative Modeling with GANs and Normalizing Flows**
   Alexandre Verine, Benjamin Negrevergne, **Muni Sreenivas Pydi** and Yann Chevaleyre
   Neural Information Processing Systems (NeurIPS), 2023.
6. **Robust Empirical Risk Minimization via Newton's Method**
   Eirini Ioannou, **Muni Sreenivas Pydi** and Po-Ling Loh
   Econometrics & Statistics, 2023.
7. **The Many Faces of Adversarial Risk: An Expanded Study**
   Muni Sreenivas Pydi and Varun Jog
   IEEE Transactions on Information Theory, 2023.
8. **The Many Faces of Adversarial Risk**
   Muni Sreenivas Pydi and Varun Jog
   Neural Information Processing Systems (NeurIPS), 2021.
9. **Adversarial Risk via Optimal Transport and Optimal Couplings**
   Muni Sreenivas Pydi and Varun Jog
   IEEE Transactions on Information Theory, 2021.
10. **Adversarial Risk via Optimal Transport and Optimal Couplings**
    Muni Sreenivas Pydi and Varun Jog
    International Conference on Machine Learning (ICML), 2020.

11. **Active Learning with Importance Sampling**
Muni Sreenivas Pydi and Vishnu Lokhande
NeurIPS Workshop on ML with Guarantees, 2019.

12. **Graph-Based Ascent Algorithms for Function Maximization**
Muni Sreenivas Pydi*, Varun Jog and Po-Ling Loh*
Allerton Conference on Communication, Control and Computing, 2018.

13. **On Consistency of Compressive Spectral Clustering**
Muni Sreenivas Pydi*, and Ambedkar Dukkipati*
IEEE International Symposium on Information Theory (ISIT), 2018.

14. **Random access retransmission scheme for power limited nodes**
Karthik Nagasubramanian, and **Muni Sreenivas Pydi**
IEEE National Conference on Communications (NCC) India, 2017.

Research Experience

Université Paris Sciences & Lettres (PSL), Paris, France
Fellow in Artificial Intelligence (LAMSADE Laboratory, Dauphine-PSL) Oct 2022 - Present

- Research on trustworthy machine learning with a focus on adversarial robustness, differential privacy and fairness.

University of Cambridge, Cambridge, UK
Visiting Student (Statistical Laboratory) May 2022 - Aug 2022

- 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

- Research on statistical consistency of graph 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

Université Paris Sciences & Lettres (PSL), Paris, France
Fellow in Artificial Intelligence (LAMSADE Laboratory, Dauphine-PSL) Oct 2022 - Present

- Lead instructor for the Machine Learning Seminar for AI4theSciences PhD program, 2023.
- Co-Instructor for "Differential Privacy for Machine Learning" course in the Masters in AI, Systems and Data (IASD) program, 2024.
- Lead instructor for "Introduction to Machine Learning", "Data Structures and Algorithms in Python", "Data Management and SQL" courses in the 'Data Science and AI for Academics' program, 2024-2025.
- Lead instructor for "Introduction to Artificial Intelligence " course in the 'Bachelor of Science in AI' program, 2025.

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

- 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.

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 radar at the Satish Dhavan Space Center.

Technical Skills

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

Invited Talks

1. **Optimal Classification under Performative Distribution Shift** August 2025
   Hosts: Prof. Nicolas Garcia Trillos (Uw-Madison), Prof. Leon Bungert (University of Würzburg), Prof. Jose Blanchet (Stanford University)
   BIRS Workshop on Mathematical Analysis of Adversarial Machine Learning, Mexico.
2. **Randomization in Adversarial Binary Classification** August 2023
   Host: Prof. Nicolas Garcia Trillos (Uw-Madison)
   Minisymposium on Adversarial robustness at the interface of analysis, geometry and statistics, International Congress on Industrial and Applied Mathematics (ICIAM 2023) Tokyo, Japan.
3. **Adversarial Robustness via Optimal Transport** June 2022
   Host: Prof. Po-Ling Loh (University of Cambridge)
   Institute of Mathematical Statistics Annual Meeting, London, UK.
4. **Theoretical Foundations of Adversarial Robustness** Apr 2022
   Host: Prof. Shuchin Aeron (Tufts University)
   Tufts ECE Graduate Seminar (online), Tufts University, USA.
5. **Theoretical Foundations of Adversarial Robustness** Jan 2022
   Host: Prof. Clement Royer (Université PSL)
   MILES (Machine Intelligence & Learning Systems) Seminar (online), PSL-Dauphine, France.
6. **Introduction to Adversarial Learning** Feb 2021
   Host: Prof. Mangal Kothari (IIT Kanpur)
   Workshop on Decision & Control: Optimal Planning, ML & Games (online), IIT Kanpur, India.
7. **On Consistency of Compressive Spectral Clustering** Aug 2018
   Host: Prof. Robert Nowak (UW-Madison)
   Summer SILO (Systems, Information, Learning & Optimization) Seminar, UW-Madison, USA.

Service

Lead Organizer of Banff International Research Station (BIRS) Workshop on Machine Learning and Statistics: From Theory to Practice, Chennai, India, January 2025.

Reviewer for Advances in Neural Information Processing Systems (NeurIPS), International Conference on Learning Representations (ICLR), 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

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.