Amartya **Sanyal**

(+49)01723842977 | amartya18x@gmail.com | https://www.amartya18x.github.io | amartya18x | @AmartyaSanyal

Professional Experience

Tenure Track Assistant Professor in Machine Learning — *Copenahgen, Denmark*
Department of Computer Science, University of Copenhagen — *August 2024-*

Affiliated Assistant Professor — *Copenahgen, Denmark*
Department of Mathematics, University of Copenhagen — *August 2024-*

Postdoctoral Fellow, Max Planck Institute for Intelligent Systems — *Tübingen, Germany*
With Prof. Bernhard Schölkopf — *April 2023 - Now*

Postdoctoral Fellow, ETH AI Center — *Zürich, Switzerland*
With Prof. Fanny Yang — *October 2021 - March 2023*

Research Assistant, University of Oxford — *Oxford, UK*
With Prof. Philip H.S. Torr — *June 2021 - September 2021*

Part Time Researcher, Facebook AI Research — *London, UK*
with Dr. Edward Grefenstette — *November 2020 - April 2021*

Education

D.Phil in Computer Science (Advisor : Dr. Varun Kanade and Dr. Philip H.S. Torr) — *Passed with Minor Corrections*
University of Oxford, St. Hugh's College — *2017 - 2021*

B.Tech. in Computer Science and Engineering (Minor in Linguistics Theory) — *CPI - 9.4/10.0*
Indian Institute of Technology, Kanpur — *2013 - 2017*

Awards

'24	**Rising Star Talk in Applied Algorithms for ML Workshop**, Paris
'23	**Rising Star in AI**, KAUST
'22	**ELLIS Member**, ELLIS Society
'21-'23	**ETH AI Center Postdoctoral Fellowships Award**, Awarded by the ETH AI Center, Zürich, Switzerland
'17-'21	**Turing Doctoral Studentship Award**, Awarded by The Alan Turing Institute, London, UK
'19-'22	**Top Reviewer Award**, NeurIPS 2022, ICML 2020, NeurIPS 2019
'14 & '16	**Academic Excellence Award**, Awarded to top 10% student, IIT Kanpur

Grants

2022	**Awarded an Hasler Stiftung Grant of 50,000 CHF**, Principal Investigator of a project on Privacy and Fairness in Machine Learning	*ETH Zürich*
2024	**Awarded NNF Startup Package 4,000,000 DKK (536,000 Euro)**, Principal Investigator	*University of Copenhagen*

Teaching

Instructor

'24	**Advanced Topics in Machine Learning**, Dept. of Computer Science, University of Copenhagen
'24	**Machine Learning B**, Dept. of Computer Science, University of Copenhagen
'23	**Advanced Topics in Machine Learning**, Dept. of Computer Science, University of Copenhagen
'22	**Guarantees in Machine Learning**, Dept. of Computer Science, ETH Zürich
'22	**Projects in Machine Learning Research**, Dept. of Computer Science, ETH Zürich

Tutor

'21	**Computational Learning Theory**, Dept. of Computer Science, University of Oxford
'19', '20	**Theory of Optimization**, Department of Engineering Science, University of Oxford
'18, '19	**Machine Learning**, Wadham College, Worcester College, Somerville College, University of Oxford
'18, '19, '20	**Machine Learning**, Dept. of Computer Science, University of Oxford
'17	**Teaching Assistant in Computational Complexity**, Department Computer Science, University of Oxford
'14	**Academic Mentor in Linear Algebra, Real Analysis and ODEs**, Indian Institute of Technology (IIT) Kanpur

Advised Students

'24- **Johanna Duëngler**, (Offical advisor) PhD Student, University of Copenhagen
'23- **Omri Ben Dov** , (Offical Co-advisor) PhD Student, Max Planck Institute for Intelligent Systems
'23- **Anmol Goel**, (Offical Co-advisor) PhD Student,ELLIS, TUDarmstadt
'23 **Yaxi Hu**, Ph.D Student, Max-Planck Institute for Intelligent Systems
'23 **Kristóf Szabó** , Master's Student in Mathematics, ETH Zürich
'22 **Francesco Pinto**, D.Phil (Ph.D) Student, University of Oxford
'22 **Piersilvio De Bartolomeis**, Master's Student in Data Science,ETH Zürich
'22 **Gizem Yüce**, Master's Student in Data Science, ETH Zürich
'22 **John Hill**, Master's Student in Computer Science, Georgia Institute of Technology
'22 **Angelo Gnazzo**, Master's Student in Mathematics, ETH Zürich
'20 **Sharan Gopal**, Master's Student in Advanced Computer Science, University of Oxford

Talks

June '24 **Applied Algorithms for ML Workshop,Rice Global University**, Paris
Nov '23 **CISPA,Helmholtz Institute**, Saarbrücken
Oct '23 **Data Science Seminar, University of Michigan**, USA
Oct '23 **META AI, Facebook**, USA
Sep '23 **Department of Electrical Engineering and Computer Science, MIT**, USA
Sep '23 **Department of Computer Science, University of Helsinki**, Finland
Feb '23 **Rising Stars in AI Symposium, KAUST**, Saudi Arabia
Dec '22 **École Polytechnique Fédérale de Lausanne**, Switzerland
Oct '22 **Max-Planck-Institut für Intelligente Systeme, Tübingen**, Germany
July '22 **The Alan Turing Institute, London**, UK
June '22 **Department of Engineering Science, University of Oxford**, UK
June '22 **Department of Computer Science, University of Edinburgh**, UK
Oct '21 **Department of Statistics, ETH Zürich**, Switzerland
Feb '21 **Department of Computer Science, Harvard University**, Boston
Nov '20 **Math Machine Learning seminar MPI MIS + UCLA, Max-Planck-Institut für Mathematik**, Germany
Nov '20 **Max-Planck-Institut für Informatik, Saarbrücken**, Germany
Oct '20 **Machine Learning and Computer Vision Group, Institute of Science and Technology, Vienna**, Austria
Oct '20 **Thoth team, Inria Grenoble Rhône-Alpes, Grenoble**, France
Sep '20 **Department of Computer Science and Engineering, Indian Institute of Technology, Hyderabad**, India
Aug '20 **Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur**, India

Academic Service

Workshop Organisation

'23 **Workshop on "Pitfalls of limited data and computation for Trustworthy ML" in ICLR 2023**,

Journal Reviewing

'24 **Journal of Privacy and Confidentiality** ,
'23 **IEEE Transactions on Pattern Analysis and Machine Intelligence**,
'22 **Transactions in Machine Learning Research**,
'20 **International Journal of Computer Vision**,

Area Chair

'24 **Artificial Intelligence and Statistics (AISTATS)**,
'23 **Artificial Intelligence and Statistics (AISTATS)**,

Conference Reviewing

'24 **ICML 2024,COLT 2024**,
'23 **NeurIPS 2023,ICLR 2024**,
'22 **NeurIPS 2022, UAI2022, AISTATS 2022, ICML 2022, ICLR 2023**,
'21 **NeurIPS 2021, AISTATS 2021, ICLR 2022, ICML 2021**,
'20 **ICLR 2021, SODA 2020, NeurIPS 2020, ICML 2020, CVPR 2020, ECCV 2020**,
'19 **NeurIPS 2019**,

Conference and Journal Publications

Provable Privacy with Non-Private Pre-Processing
Yaxi Hu, Amartya Sanyal, Bernhard Schölkopf
International Conference on Machine Learning, 2024

The Role of Learning Algorithms in Collective Action
Omri Ben-Dov, Jake Fawkes, Samira Samadi, Amartya Sanyal
International Conference on Machine Learning, 2024

Sample-efficient private data release for Lipschitz functions under sparsity assumptions
Konstantin Donhauser, Johan Lokna, Amartya Sanyal, March Boedihardjo, Robert Hönig, Fanny Yang
International Conference on Artificial Intelligence and Statistics (AISTATS) 2024
Theory and Practice of Differential Privacy (TPDP). 2023

PILLAR: How to make Semi-private learning more effective
Francesco Pinto, Yaxi Hu, Fanny Yang, Amartya Sanyal
IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) 2024
Theory and Practice of Differential Privacy (TPDP), 2023

Can semi-supervised learning use all the data effectively? A lower bound perspective
Gizem Yüce, Alenxandru Tifrea, Amartya Sanyal, Fanny Yang
Neural Information Processing Systems (NeurIPS) Spotlight Paper, 2023

Certifying Ensembles: A General Certification Theory with $\mathcal{S}$-Lipschitzness
Aleksander Petrov, Francisco Eiras, Amartya Sanyal, Philip H.S. Torr, Adel Bibi
International Conference on Machine Learning (ICML), 2023

How robust are pre-trained models to distribution shift?
Yuge Shi, Imant Daunhawer, Julia E. Vogt, Philip H.S. Torr, Amartya Sanyal
International Conference on Learning Representations (ICLR), 2023

A law of adversarial risk, interpolation, and label noise
Daniel Paleka, Amartya Sanyal
International Conference on Learning Representations (ICLR), 2023

Make Some Noise: Reliable and Efficient Single-Step Adversarial Training
Pau Jorge, Amartya Sanyal, Adel Bibi, Ricardo Volpi, Gregory Rogez, Puneet K. Dokania, Philip H. S. Torr
Advanced in Neural Information Processing Systems (NeurIPS), 2022

How unfair is private learning?
Amartya Sanyal, Yaxi Hu, Fanny Yang
Conference on Uncertainty in Artificial Intelligence (UAI) Oral Paper, 2022

Open Problem: Do you pay for Privacy in Online learning?
Amartya Sanyal, Giorgia Ramponi
Conference on Learning Theory (COLT), Open Problem, 2022

How Benign is Benign Overfitting ?
Amartya Sanyal, Varun Kanade, Philip H.S. Torr, Puneet K. Dokania
International Conference on Learning Representations (ICLR), Spotlight Paper, 2021

Progressive Skeletonization: Trimming more fat from a network at initialization
Pau Jorge, Amartya Sanyal, Harkirat S. Behl, Philip H. S. Torr, Gregory Rogez, Puneet K. Dokania
International Conference on Learning Representations (ICLR), 2021

Stable Rank Normalization for Improved Generalization in Neural Networks and GANs
Amartya Sanyal, Philip H.S. Torr, Puneet K. Dokania
International Conference on Learning Representations (ICLR), Spotlight Paper, 2020

The Intriguing Effects of Focal Loss on the Calibration of Deep Neural Networks
Jishnu Mukhoti, Viveka Kulharia, Amartya Sanyal, Stuart Golodetz, Philip H. S. Torr, Puneet K. Dokania
Advances in Neural Information Processing Systems (NeurIPS), 2020

TAPAS: Tricks to Accelerate (encrypted) Prediction As a Service
Amartya Sanyal, Matt Kusner, Adria Gascon, Varun Kanade
International Conference on Machine Learning (ICML), 2018

Optimizing non-decomposable measures with deep networks
Amartya Sanyal, Pawan Kumar, Purushottam Kar, Sanjay Chawla, Fabrizio Sebastiani
Springer,Machine Learning. 2018

A Hybrid Deep Architecture for Face Recognition in Real-Life Scenario
Amartya Sanyal, Ujjwal Bhattacharya, Swapan K. Parui
Lecture Notes in Computer Science (Vol. 10481), 2016

Workshop Publications and Preprints

On the Growth of Mistakes in Differentially Private Online Learning: A Lower Bound Perspective
Daniil Dmitriev, Kristóf Szabó, Amartya Sanyal
Conference on Learning Theory, 2024

Corrective Machine Unlearning
Shashwat Goel, Ameya Prabhu, Philip Torr, Ponnurangam Kumaraguru, Amartya Sanyal
ICLR Workshop on Data-Centric Machine Learning Research. 2024

How robust accuracy suffers from certified training with convex relaxations
Piersilvio De Bartolomeis, Jacob Clarysse, Fanny Yang, Amartya Sanyal
NeurIPS 2022: Workshop on Understanding Deep Learning Through Empirical Falsification Contributed Talk, 2022

Semi-private learning via low dimensional structures
Yaxi Hu, Francesco Pinto, Amartya Sanyal, Fanny Yang
Third Workshop on Seeking Low-Dimensionality in Deep Neural Networks, 2023

Catastrophic Overfitting is a bug but also a feature
Guillermo Ortiz-Jimenez, Pau Jorge, Amartya Sanyal, Adel Bibi, Puneet Dokania, Pascal Frossard, Gregory Rogez, Philip H. S. Torr
ICML 2022: Workshop on New Frontiers In Adversarial Machine Learning, 2022

Robustness via Deep Low Rank Representations
Amartya Sanyal, Varun Kanade, Philip H.S. Torr, Puneet Dokania
ICML 2018: Workshop on Theory and Application of Deep Generative Models, 2018

Multiscale sequence modeling with a learned dictionary
Bart Merriënboer, Amartya Sanyal, Hugo Larochelle, Yoshua Bengio
ICML 2017: Workshop on Machine Learning in Speech and Language Processing, 2017