Mahalakshmi Sabanayagam

Email | Google Scholar | Website | Github | LinkedIn

Research Interest

I am interested in the theory of machine/deep learning, primarily in understanding its connection to kernels and the interplay between adversarial robustness and optimization. I am also interested in graph based learning problems.

Education

Ph.D. in Computer Science — August 2021 – Present
Technical University of Munich, Germany
Advisor: *Prof. Debarghya Ghoshdastidar*

Master of Science, Informatics — October 2018 – June 2021
Technical University of Munich, Germany — *CGPA: 1.3 (best of 1.0)*

Bachelor of Technology, Computer Science & Engineering — July 2011 – May 2015
National Institute of Technology, Trichy, India — *CGPA: 9.37 (best of 10)*

Academic / Industry Experience

Research Visitor, CSIRO, Australia — August 2024 – November 2024

Working with *Dr. Cheng Soon Ong* and *Dr. Russell Tsuchida*, on theoretical analysis of adversarial robustness of probabilistic models.

Research Visitor, New York University, USA — March 2023 – June 2023

Worked with *Prof. Julia Kempe*, on theoretical analysis of adversarial robustness of neural networks, and together with *Prof. Andrew Gordon Wilson* on robustness to distributional shifts under Bayesian inference.

Computer Scientist 1, Adobe Systems, India — July 2015 – September 2018

Developed a robust OS agnostic (Mac/Windows) framework for Dreamweaver, with HiDPI adaptation. Upgraded Chromium Embeded Framework (CEF) with custom optimization for messaging queue and memory.

Recognized as a top contributor and was awarded two early promotions - *Member of Technical Staff 2* in January 2017 and *Computer Scientist 1* in January 2018.

Research Intern, Samsung R&D Institute, India — May 2014 – July 2014

Implemented a module for secure log-out in Android Browser of Samsung. Worked on improving the efficiency of Optical Character Recognition using Tesseract and OpenCV.

Publications

11. **Exact Certification of (Graph) Neural Networks Against Label Flipping.** *Mahalakshmi Sabanayagam**, Lukas Gosch*, Stephan Günnemann, Debarghya Ghoshdastidar. **Spotlight** at International Conference on Learning Representations ***(ICLR 2025)*** [paper][code]

10. **Provable Robustness of (Graph) Neural Networks Against Data Poisoning and Backdoors.** Lukas Gosch*, *Mahalakshmi Sabanayagam**, Debarghya Ghoshdastidar, Stephan Günnemann. **Oral, Best Paper Award** at New Frontiers of Adversarial Machine Learning Workshop, NeurIPS ***(AdvML-Frontiers NeurIPS 2024)*** [paper][code]

9. **Kernels, Data & Physics.** Francesco Cagnetta, Deborah Oliveira, *Mahalakshmi Sabanayagam*, Nikolaos Tsilivis, Julia Kempe. At Journal of Statistical Mechanics: Theory and Experiment ***(JSTAT Lecture Notes 2024)*** [paper]

8. **Robust Feature Inference: A Test-time Defense Strategy using Spectral Projections.** Anurag Singh*, *Mahalakshmi Sabanayagam**, Krikamol Muandet, Debarghya Ghoshdastidar. At Transactions on Machine Learning Research ***(TMLR 2024)*** [paper][code]

*Equal Contribution

7. **Unveiling the Hessian's Connection to the Decision Boundary.** *Mahalakshmi Sabanayagam*, Freya Behrens, Urte Adomaityte, Anna Dawid. At Mathematics of Modern Machine Learning Workshop, NeurIPS ***(M3L NeurIPS 2023)*** [paper][code]

6. **Analysis of Convolutions, Non-linearity and Depth in Graph Neural Networks using Neural Tangent Kernel.** *Mahalakshmi Sabanayagam*, Pascal Esser, Debarghya Ghoshdastidar. At Transactions on Machine Learning Research ***(TMLR 2023)*** [paper][code]

5. **Improved Representation Learning Through Tensorized Autoencoders.** Pascal Esser*, Satyaki Mukherjee*, *Mahalakshmi Sabanayagam**, Debarghya Ghoshdastidar. At International Conference on Artificial Intelligence and Statistics ***(AISTATS 2023)*** [paper][code]

4. **Analysis of Graph Convolution Networks using Neural Tangent Kernels.** *Mahalakshmi Sabanayagam*, Pascal Esser, Debarghya Ghoshdastidar. At MLG workshop, European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases ***(ECML PKDD 2022)*** [paper][code]

3. **Graphon based Clustering and Testing of Networks: Algorithms and Theory.** *Mahalakshmi Sabanayagam*, Leena Chennuru Vankadara, Debarghya Ghoshdastidar. At International Conference on Learning Representations ***(ICLR 2022)*** [paper][code]

2. **Rough Set-based Feature Selection for Credit Risk Prediction using Weight Adjusted Boosting Ensemble Method.** Sivasankar Elango, Selvi Chandran, *Mahalakshmi Sabanayagam.* At Journal of Soft Computing 2019 [paper]

1. **Cross Domain Sentiment Analysis Using Different Machine Learning Techniques.** *Mahalakshmi Sabanayagam*, Sivasankar Elango. At Fifth International Conference on Fuzzy and Neuro Computing ***(FANCCO 2015)*** and as poster in Grace Hopper Celebration India ***(GHCI 2016)*** [paper]

Preprints / Under Review

3. **Generalization Certificates for Adversarially Robust Bayesian Linear Regression.** *Mahalakshmi Sabanayagam*, Russell Tsuchida, Cheng Soon Ong, Debarghya Ghoshdastidar.

2. **Cluster Specific Representation Learning.** *Mahalakshmi Sabanayagam*, Omar Al-Dabooni, Pascal Esser

1. **Machine learning-based image detection for lensless microscopy in life science.** *Mahalakshmi Sabanayagam*, Jan Brunckhorst, Andreas Pirchner, Nikhitha Radhakrishna Naik [link]

Research Activities

- *Workshop:* Understanding Generalization in Deep Learning, Burghausen, Germany — February 19-21, 2025
- *Workshop:* AI in Science Conference, Canberra, Australia — November 6, 2024
- *Summer School:* Statistical Physics & Machine Learning, Cargese, France — August 1-12, 2023
- *Workshop:* Physics for Neural Networks, Center for Theoretical Science, Princeton — April 17-19, 2023
- *Summer School:* Statistical Physics & Machine Learning, Les Houches, France — July 4-29, 2022
- *Reviewer:* ICLR 2025, NeurIPS 2024, TMLR 2024, AISTATS 2023

Teaching / Student Jobs

- *Teaching Assistant* for Seminar on Theoretical Advances in Deep Learning (WS 2022/23, WS 2023/24), Statistical Foundations of Learning (SS 2022), Analysis of new phenomena in machine/deep learning (SS 2022, SS 2023,SS 2024), Gems of Informatics 3: Modelling and analysis of graphs (WS 2021/22, WS 2022/23), Efficient Algorithms & Data Structures (WS 2020/21)

- *Research Assistant* in Certifiable AI at Fraunhofer-Institute, Munich (Sept 2020 – Feb 2021): Worked on novel ways to quantify risk in object detectors

- *Working Student* in Innovation Department at Osram Gmbh, Munich (Sept 2019 – Dec 2019): Developed faster RCNN and YOLO based models for detection, identification and tracking of multiple traffic objects

Awards & Honors

- **Best Paper Award** at the 3rd AdvML-Frontiers Workshop, NeurIPS 2024
- **3rd** price in EMCR talk at AI in Science Conference 2024, Canberra, with a cash award of 1,000 AUD
- *Funding:* TUM-GS Internationalization Support of 3,000 Euro for the NYU research visit in 2023
- Largest sustainability impact award by **Siemens AI@sustainability Hackathon, 2020** for the AI solution towards finding new strategies that reduce the spread of COVID-19
- **2nd** place in Female Tech Leaders Hackathon on **Introduction to Big Data: COVID-19 and its Global Effects, 2020** for analysing COVID-19 related tweets and the impact on equities
- Finalist in **Mobility Innovation Competition @ Campus, 2019** by Zentrum Digitalisierung Bayern
- **O.P. Jindal Engineering and Management Scholarship, 2012** one among 100 students all over India
- **Bachelor's Study scholarship** from NLC for the period 2011 – 2015
- Bronze medal (national level) and 1^{st} in the city in **National Cyber Olympiad, 2007**

Technical Skills

Languages: C++ (Proficient), Python (Proficient), Java (Good)
Technologies: Tensorflow, Pytorch, JAX, NetworkX, Chromium Embedded Framework, OpenCV, AWS, Git