Anshul **Nasery**

PhD Student, University of Washington

@ anshulnasery@gmail.com Homepage Github Google Scholar

Research Interests

I work on practical advances towards secure, robust and efficient AI systems informed by thorough empirical analyses.

Education

Ongoing | **University of Washington**
Sept 2023 | PhD in Computer Science
Advisor: Prof. Sewoong Oh

Aug 2021 | **Indian Institute of Technology, Bombay** **GPA: 9.58/10**
Jul 2017 | Bachelor of Technology (With Honors) in Computer Science and Engineering, Minor in Statistics

Industrial Research Experience

Jul 2023 | **Google Research** **Bangalore, India**
Jul 2021 | *Pre-Doctoral Researcher | Advisor: Dr. Prateek Jain, Dr. Praneeth Netrapalli*
Worked on robustness and inference efficiency of deep networks [ICLR'23, CVPR-W'24].

Jul 2020 | **Adobe Research** **Bangalore, India**
Apr 2020 | *Research Intern | Advisor: Dr. Balaji Vasan Srinivasan*
Worked on Multimodal Question Answering [NAACL'21, US Patent].

Selected Publications

Security

[S.1] **Scalable Fingerprinting of Large Language Models** [🔗]
Anshul Nasery, Jonathan Hayase, Creston Brooks, Peiyao Sheng, Himanshu Tyagi, Pramod Viswanath, Sewoong Oh
Spotlight *at 39th Conference on Advances in Neural Information Processing Systems* **[NeurIPS'25]**

[S.2] **Are Robust LLM Fingerprints Adversarially Robust?** [🔗]
Anshul Nasery, Edoardo Contente, Alkin Kaz, Pramod Viswanath, Sewoong Oh
Under Review **[Pre-print]**

[S.3] **Towards Secure Model Sharing with Approximate Fingerprints** [🔗]
Anshul Nasery, Sewoong Oh
Reliable and Responsible Foundation Models, ICML 2025 **[ICML-W'25]**

Robustness

[R.1] **Learning an Invertible Mapping can Mitigate Simplicity Bias** [🔗]
Sravanti Addepalli*, **Anshul Nasery***, R Venkatesh Babu, Praneeth Netrapalli, Prateek Jain
International Conference on Learning Representations, 2023 **[ICLR'23]**

[R.2] **DAFT: Distilling Adversarially Finetuned Teachers for better OOD generalization** [🔗]
Anshul Nasery, Sravanti Addepalli, Praneeth Netrapalli, Prateek Jain
Principles of Distribution Shifts Workshop, ICML 2022 **[ICML-W'22]**

[R.3] **Training for the Future: A Simple Gradient Interpolation loss to Generalize Along Time** [🔗]
Anshul Nasery*, Soumyadeep Thakur*, Vihari Piratla, Abir De, Sunita Sarawagi
34th Conference on Advances in Neural Information Processing Systems **[NeurIPS'21]**

Efficiency

[E.1] **PLeaS – Merging Models with Permutations and Least Squares** [🔗]
Anshul Nasery*, Jonathan Hayase*, Pang Wei Koh, Sewoong Oh
IEEE / CVF Computer Vision and Pattern Recognition Conference, 2025 **[CVPR'25]**

[E.2] **What if Neural Networks had SVDs?** [🔗]
Alexander Mathiasen, Frederik Hvilshøj, Jakob Rødsgaard Jørgensen, **Anshul Nasery**, Davide Mottin
Spotlight *at 33rd Conference on Advances in Neural Information Processing Systems* **[NeurIPS'20]**

[E.3] **End-to-End Neural Network Compression via $\frac{\ell_1}{\ell_2}$ Regularized Latency Surrogates** [🔗]
Anshul Nasery, Hardik Shah, Arun Suggala, Prateek Jain
Oral *at Mobile AI Workshop at CVPR 2024* **[CVPR-W'24]**

Applications

[A.1] **Peekaboo: Interactive Video Generation via Masked-Diffusion** [🔗]
Anshul Nasery*, Yash Jain*, Vibhav Vineet, Harkirat Behl
IEEE / CVF Computer Vision and Pattern Recognition Conference, 2024 **[CVPR'24]**

[A.2] **MIMOQA: Multimodal Input Multimodal Output Question Answering** [🔗]
Hrituraj Singh, **Anshul Nasery***, Denil Mehta*, Jatin Lamba, Aishwarya Agarwal, Balaji Vasan
2021 Conference of the North American Chapter of the Association for Computational Linguistics **[NAACL'21]**

Selected Research Projects

Robust and Scalable Fingerprinting for LLMs May '24 – Present

Advisors: Prof. Sewoong Oh

- Investigated techniques for secure model sharing by embedding fingerprints by fine-tuning large language models.
- Proposed a novel sampling technique, adding up to 25,000 fingerprints with minimal utility drop [Spotlight at NeurIPS'25].
- Developed adaptive attacks achieving perfect attack success rates against 10 recent fingerprinting schemes [Preprint].
- Proposed embedding statistical signals and using approximate detection for secure fingerprinting [ICML-W'25].

Out-of-Domain Robustness of Neural Nets Sept '21 – June '23

Advisors: Dr. Prateek Jain, Dr. Praneeth Netrapalli

- Studied the connection between simplicity bias and out-of-distribution (OOD) generalization of neural networks, empirically analyzing the mechanisms for the former through controlled experiments on synthetic data.
- Proposed Feature Reconstruction Regularizer, obtaining a 1% gain in accuracy over SOTA methods on DomainBed. [ICLR'23]
- Combined adversarial fine-tuning and knowledge distillation to boost the OOD robustness of small models. [ICML-W'22]

Model merging for efficient ensembles Nov '23 – May '24

Advisors: Prof. Sewoong Oh, Prof. Pang Wei Koh

- Worked on model merging for multi-task learning. Extended Git Re-Basin to produce merged models of varying sizes.
- Proposed a novel feature adjustment step to distill knowledge into a merged model with minimal data requirements.
- Demonstrated empirical gains of up to 13% over state-of-the-art merging methods for various tasks. [CVPR'25]

Inference Efficient ML Models Jul '21 – Jul '23

Advisors: Dr. Prateek Jain, Dr. Praneeth Netrapalli, Dr. Gaurav Aggarwal

- **NAS.** Proposed a novel regularizer to minimize FLOPs and on-device latency for vision and language models. Achieved a 15% reduction in FLOPs on MobileNetV3 and a 50% reduction on BERT with minimal performance drop [CVPR-W'24].
- **Conditional Computation.** Obtained a 1% gain in ImageNet accuracy for MobileNetV2 by introducing decision trees to route examples. Introduced a skip-and-branch architecture for 25% savings in amortized FLOPs with MobileNetV3.

Other Projects

Training for the Future Jul '20 – Jul '21

Advisor: Prof. Sunita Sarawagi

- Proposed a gradient-based smoothness regularizer for better temporal generalization under gradual drift. [NeurIPS'21]

Controllable Video Generation Oct '23 – Dec '23

Advisors: Dr. Vibhav Vineet, Dr. Harkirat Behl

- Proposed a training-free method for spatio-temporally controlling the outputs of any video generation model [CVPR'24].

Multimodal Question Answering Apr '20 – Jul '20

Advisor: Dr. Balaji Vasan Srinivasan

- Proposed task definition, dataset and baselines for question answering with multimodal inputs and outputs [NAACL'21].

Efficient Products of Householder Matrices Dec '19 – Jan '20

Advisor: Prof. Davide Mottin

- Implemented efficient CUDA kernels for parallelized multiplication of products of Householder matrices [NeurIPS'20].

Theoretical Analysis of Transfer Learning Jan '21 – Apr '21

Advisor: Prof. Nutan Limaye

- Formulated transfer learning as a three-player adversarial game to get learning bounds in a universal learning framework.

Academic Achievements

- Awarded Institute Academic Prize for exceptional academic performance (top 10% of class) at IIT Bombay in 2017–2018.
- Ranked **137** among 110,000 candidates in JEE Advanced 2017 and **265** among 1.5 million candidates in JEE Main 2017.
- Placed among the **top 35 students** in the Indian National Astronomy Olympiad 2017, and qualified for the Indian National Olympiad in Informatics, the Indian National Physics Olympiad, and the Indian National Chemistry Olympiad (2017).

Key Courses Undertaken

Machine Learning	Theoretical ML, Advanced ML, Natural Language Processing, Interactive Learning
Math and Statistics	Linear Algebra, Statistical Inference, Probability and Measure Theory, Regression Analysis

Service

- Reviewer for ICML (2022, 2024), NeurIPS (2022–2025), ICLR (2022, 2023, 2025), CVPR (2023, 2024), COLM (2024).
- Teaching assistant for a graduate-level course on Advanced ML at the University of Washington; undergraduate courses on Artificial Intelligence, Machine Learning, and Quantum Mechanics at IIT Bombay.
- Mentored students from underrepresented communities for grad school applications at UW.