3401 Walnut Street
Philadelphia, PA 19104
(203) 807-2033
arobey1@seas.upenn.edu
https://arobey1.github.io/

Alexander Robey

Education

2018–present **PhD, Electrical and Systems Engineering**, *University of Pennsylvania*, Philadelphia, PA..

2014-2018 **Bachelor of Science, Engineering**, *Swarthmore College*, Swarthmore, PA..

2014-2018 **Bachelor of Arts, Mathematics**, *Swarthmore College*, Swarthmore, PA..

Work Experience

2022-2023 Student researcher, Google Cloud AI.

2022 Research Intern, Google Cloud AI.

2017 Research Intern, Center for Applied Scientific Computing, Lawrence Livermore National Laboratory.

2016, 2018 Research Assistant, Department of Engineering, Swarthmore College.

Refereed Conference Papers

2022 Allan Zhou, Fahim Tajwar, **Alexander Robey**, Tom Knowles, George J. Pappas, Hamed Hassani, and Chelsea Finn. Do Deep Networks Transfer Invariances across Classes? In *International Conference on Learning Representations*, 2022.

2022 Anton Xue, Lars Lindemann, **Alexander Robey**, Hamed Hassani, George J. Pappas, and Rajeev Alur. Chordal Sparsity for Lipschitz Constant Estimation of Deep Neural Networks. In *2022 61st IEEE Conference on Decision and Control (CDC)*. IEEE, 2022.

2022 Stephen Tu, **Alexander Robey**, Tingnan Zhang, and Nikolai Matni. On the Sample Complexity of Stability Constrained Imitation Learning. In *Learning for Dynamics and Control*. PMLR, 2022.

2022 **Alexander Robey**, Luiz F. O. Chamon, George J. Pappas, and Hamed Hassani. Probabilistically Robust Learning: Balancing Average-and Worst-case Performance. In *International Conference on Machine Learning*. PMLR, 2022.

2022 Cian Eastwood*, **Alexander Robey***, Shashank Singh, Julius von Kügelgen, Hamed Hassani, George J. Pappas, and Bernhard Schölkopf. Probable domain generalization via quantile risk minimization. *Advances in Neural Information Processing Systems*, 2022.

2021 **Alexander Robey***, Luiz F. O. Chamon*, George J. Pappas, Hamed Hassani, and Alejandro Ribeiro. Adversarial Robustness with Semi-Infinite Constrained Learning. In *Advances in Neural Information Processing Systems*, 2021.

2021 **Alexander Robey**, George J. Pappas, and Hamed Hassani. Model-Based Domain Generalization. In *Advances in Neural Information Processing Systems*, 2021.

2021 **Alexander Robey**, Lars Lindemann, Stephen Tu, and Nikolai Matni. Learning Robust Hybrid Control Barrier Functions for Uncertain Systems. *IFAC Conference on Analysis and Design of Hybrid Systems*, 2021.

2021 **Alexander Robey**, Arman Adibi, Brent Schlotfeldt, George J. Pappas, and Hamed Hassani. Optimal Algorithms for Submodular Maximization with Distributed Constraints. In *Learning for Dynamics and Control*. PMLR, 2021.

2021 Lars Lindemann, Haimin Hu, **Alexander Robey**, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning Hybrid Control Barrier Functions from Data. *Conference on Robot Learning*. PMLR, 2021.

2020 **Alexander Robey***, Haimin Hu*, Lars Lindemann, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning Control Barrier Functions from Expert Demonstrations. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3717–3724. IEEE, 2020.

2019 Mahyar Fazlyab, **Alexander Robey**, Hamed Hassani, Manfred Morari, and George Pappas. Efficient and Accurate Estimation of Lipschitz Constants for Deep Neural Networks. In *Advances in Neural Information Processing Systems*, pages 11427–11438, 2019.

Journal Papers

2022 Edgar Dobriban, Hamed Hassani, David Hong, and **Alexander Robey**. Provable Tradeoffs in Adversarially Robust Classification. *IEEE Transactions on Information Theory*. IEEE, 2022.

2018 **Alexander Robey** and Vidya Ganapati. Optimal Physical Preprocessing for Example-based Super Resolution. *Optics Express*, volume 26, pages 31333–31350. Optical Society of America, 2018.

Preprints

2022 Haoze Wu*, Teruhiro Tagomori*, **Alexander Robey***, Fengjun Yang*, Nikolai Matni, George J. Pappas, Hamed Hassani, Corina Pasareanu, and Clark Barrett. Toward certified robustness against real-world distribution shifts. *arXiv preprint arXiv:2206.03669*, 2022.

2021 Lars Lindemann, **Alexander Robey**, Lejun Jiang, Stephen Tu, and Nikolai Matni. Learning Robust Output Control Barrier Functions from Safe Expert Demonstrations. *arXiv preprint arXiv:2111.09971*, 2021.

2020 **Alexander Robey**, Hamed Hassani, and George J. Pappas. Model-Based Robust Deep Learning. *arXiv preprint arXiv:2005.10247*, 2020.

Patents

2020 **Alexander Robey**, Hamed Hassani, and George J Pappas. Model-Based Robust Deep Learning, 2020. United States Provisional Patent 63/034,355.

Fellowships & Awards

2022 *Outstanding Reviewer Award*, ICML 2022.

2021 *Outstanding Reviewer Award*, NeurIPS 2021.

2021 *Outstanding Reviewer Award*, ICLR 2021.

2020 *Outstanding Reviewer Award*, ICML 2020.

2020 *Teaching Assistant of the Year*, Department of Electrical and Systems Engineering, University of Pennsylvania.

2018 *Dean's Fellowship*, Department of Electrical and Systems Engineering, University of Pennsylvania.

2016 *Summer Undergraduate Research Fellowship*, Department of Engineering, Swarthmore College.

Professional Activities

Organizing

2022 ECCV workshop on *Adversarial Robustness in the Real World*.

2021 ICCV workshop on *Adversarial Robustness in the Real World*.

Reviewing (conferences)

Neural Information Processing Systems (NeurIPS)

International Conference on Machine Learning (ICML)

International Conference on Learning Representations (ICLR)

The AAAI Conference on Artifical Intelligence (AAAI)

International Conference on Cyber-Physical Systems (ICCPS)

Learning for Dynamics and Control (L4DC)

Conference on Decision and Control (CDC)

American Control Conference (ACC)

International Conference on Computer Vision (ICCV)

European Conference on Computer Vision (ECCV)

International Symposium on Information Theory (ISIT)

Reviewing (journals)

Journal of Machine Learning Research (JMLR)
IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI)
IEEE Robotics and Automation Letters
IEEE Transactions on Neural Networks and Learning Systems
Transactions on Automatic Control (TAC)
SIAM Journal on Mathematics of Data Science (SIMODS)
Springer Nature Journal on Machine Learning
Transactions on Machine Learning Research (TMLR)

Reviewing (workshops & special tracks)

2023 AAAI special track on *Safe and Robust AI*.
2022 NeurIPS workshop on *Distribution Shifts*.
2022 NeurIPS workshop on *Robustness in Sequence Modeling*.
2022 ECCV workshop on *Out-Of-Distribution Generalization in Computer Vision*.
2022 ECCV workshop on *Adversarial Robustness in the Real World*.
2022 ICML workshop on *Adversarial Machine Learning Frontiers*.
2021 NeurIPS workshop on *Distribution Shifts: Connecting Methods and Applications*.
2021 ICCV workshop on *Adversarial Robustness in the Real World*.
2020 ECCV workshop on *Adversarial Robustness in the Real World*.

Technical Skills

Programming languages: Python, MATLAB, JavaScript, HTML, CSS, R, C/C++, SQL (Postgres), Verilog HDL, LaTeX

Frameworks: Pytorch, TensorFlow, Jax, Django, Slurm

Teaching Experience

Spring 2022 ENGR 56: *Modeling and Optimization for Engineering*, Swarthmore College (Guest Lecturer)
Spring 2021 ESE 605: *Modern Convex Optimization*, University of Pennsylvania (Teaching Assistant)
Spring 2020 ESE 290: *Introduction to Research Methodologies*, University of Pennsylvania (Mentor)
Fall 2020 ESE 530: *Elements of Probability Theory*, University of Pennsylvania (Teaching Assistant)
Fall 2019 ESE 530: *Elements of Probability Theory*, University of Pennsylvania (Teaching Assistant)
Spring 2018 ENGR 019: *Numerical Methods for Engineering Applications*, Swarthmore College (Teaching Assistant)
Fall 2017 ENGR 011: *Electrical Circuit Analysis*, Swarthmore College (Teaching Assistant)
Spring 2017 ENGR 012: *Linear Physical Systems Analysis*, Swarthmore College (Teaching Assistant)
Fall 2016 ENGR 011: *Electrical Circuit Analysis*, Swarthmore College (Teaching Assistant)
Spring 2016 ENGR 006: *Engineering Mechanics*, Swarthmore College (Teaching Assistant)

Selected Talks

Oct. 2022 *Learning Under Robustness Constraints*, INFORMS Annual Meeting, Indianapolis, IN, USA.
July 2022 *Probabilistically Robust Learning: Balancing Worst- and Average-case Performance*, International Conference on Machine Learning (ICML), Baltimore, MD, USA.
Mar. 2022 *Probabilistically Robust Learning: Balancing Worst- and Average-case Performance*, The Institute for Learning-enabled Optimization at Scale (TILOS), Univeristy of California, San Diego, San Diego, CA, USA (virtual).
Mar. 2022 *Toward Robust, Generalizable Deep Learning*, Guest Lecture in ENGR 056: Optimization and Modeling, Swarthmore College, Swarthmore, PA, USA.
Dec. 2021 *Model-Based Domain Generalization*, CDC 2021 Workshop on Robust Deep Learning-Based Control, Austin, TX, USA (virtual).
Oct. 2021 *Robustness against Natural Variation: Theory and Practice*, GRASP SFI Seminar, University of Pennsylvania, Philadelphia, PA, USA.

Sept. 2021 *A Critique of "Generalization in Adversarially Robust Deep Learning"*, NSF-Simons Math of Deep Learning (MoDL) annual meeting, Simons Foundation, New York, NY, USA.

Sept. 2021 *Robustness against Natural Variation: Theory and Practice*, NSF-Simons THEORINET Seminar, Baltimore, MD, USA (virtual).

July 2021 *Learning Robust Hybrid Control Barrier Functions for Uncertain Systems*, 7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), Brussels, Belgium (virtual).

Apr. 2021 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, Italian Conference on CyberSecurity (ITASEC), AI for Security and Security for AI Workshop (virtual).

Mar. 2021 *Model-Based Domain Generalization*, NSF-Simons Math of Deep Learning (MoDL) seminar (virtual).

Dec. 2020 *Learning Control Barrier Functions from Expert Demonstrations*, 59^{th} IEEE Conference on Decision and Control (CDC 2020), Jeju Island, Korea (virtual).

Nov. 2020 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, Intel, Santa Clara, CA, USA (virtual).

Oct. 2020 *Generalizing to Natural Out-of-Distribution Data*, C3.ai Workshop on the Analytical Foundations of Deep Learning (virtual).

Sept. 2020 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, Intel, Santa Clara, CA, USA (virtual).

Sept. 2020 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, Data Augmentation and Equivariance Workshop, University of Pennsylvania, Philadelphia, PA, USA (virtual).

Aug. 2020 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, European Conference on Computer Vision (ECCV) workshop on Adversarial Robustness in the Real World, Glasgow, Scotland (virtual).

July 2020 *Model-Based Robust Deep Learning*, Stanford University, Stanford, CA, USA (virtual).

Dec. 2019 *Efficient and Accurate Estimation of Lipschitz Constants of Deep Neural Networks*, Spotlight talk at Neural Information Processing Systems (NeurIPS), Vancouver, Canada.

May 2018 *Computationally Expediting Fourier Ptychographic Miscroscopy*, Research Showcase, Swarthmore College, Swarthmore, PA, USA.

Selected Poster Presentations

Sept. 2022 *Probabilistically Robust Learning: Balancing Average and Worst-case Performance*, NSF-Simons Mathematics of Deep Learning (MoDL) annual meeting, Simons Foundation, New York, NY, USA.

Sept. 2022 *Probabilistically Robust Learning: Balancing Average and Worst-case Performance*, The Institute for Emerging CORE Methods in Data Science (EnCORE) annual meeting (virtual).

July 2022 *Probabilistically Robust Learning: Balancing Average and Worst-case Performance*, International Conference on Machine Learning (ICML) 2022.

July 2022 *Toward Certified Robustness Against Real-World Distribution Shifts*, International Conference on Machine Learning (ICML) workshop on Formal Verification of Machine Learning, Baltimore, MD, USA.

Apr. 2022 *Do Deep Networks Transfer Invariance Across Classes?*, International Conference on Learning Representations (ICLR) 2022.

Dec. 2021 *Adversarial Robustness via Semi-Infinite Constrained Learning*, Neural Information Processing Systems (NeurIPS) 2021.

Dec. 2021 *Model-Based Domain Generalization*, Neural Information Processing Systems (NeurIPS) 2021.

Sept. 2021 *Model-Based Domain Generalization*, NSF-Simons Mathematics of Deep Learning (MoDL) annual meeting, Simons Foundation, New York, NY, USA.

July 2021 *Model-Based Robust Deep Learning: Generalizing to Natural Out-of-Distribution Data*, International Conference on Machine Learning (ICML) Workshop on Uncertainty and Robustness in Deep Learning (virtual).

June 2021 *Optimal Algorithms for Submodular Maximization with Distributed Constraints*, Learning for Dynamics and Control (L4DC), Zurich, Switzerland (virtual).

Nov. 2020 *Learning Hybrid Control Barrier Functions from Data*, Conference on Robot Learning (CoRL), Boston, MA, USA (virtual).

Dec. 2019 *Efficient and Accurate Estimation of Lipschitz Constants of Deep Neural Networks*, Neural Information Processing Systems (NeurIPS) 2019, Vancouver, Canada.

Aug. 2017 *Quantifying the Impact of Factors Affecting Communication Performance*, Lawrence Livermore National Laborary (LLNL), Livermore, CA, USA.

Sept. 2016 *Bird-Window Collision Prevention*, Sigma Xi Poster Session, Swarthmore College, Swarthmore, PA, USA.