Anton Xue

antonxue@seas.upenn.edu
https://antonxue.github.io/

Last updated October 10, 2024

Research Interests

I will make ML systems safe and interpretable using formal methods, control theory, and optimization.

Education

2019 – ◇ **University of Pennsylvania, Ph.D. in Computer Science**
Advisors: Rajeev Alur and Eric Wong
Expected graduation: Spring 2025

2015 – 2019 ◇ **Yale University, B.S. in Computer Science and Mathematics**
Advisor: Ruzica Piskac
Double major, undergraduate research on program analysis and Haskell.

Awards

2023 ◇ Amazon Web Services grant to the University of Pennsylvania ASSET fund

2019 ◇ University of Pennsylvania ENIAC Fellowship

2019 ◇ Yale Computer Science Award

2019 ◇ National Science Foundation Graduate Research Fellowship

2016 ◇ Yale College Freshman Summer Research Fellowship

Publications

Preprints

1. H. Jin, S. Havaldar, C. Kim, *et al.*, "The FIX Benchmark: Extracting Features Interpretable to eXperts," *arXiv preprint arXiv:2409.13684*, 2024.
2. A. Xue, A. Khare, R. Alur, S. Goel, and E. Wong, "Logicbreaks: A Framework for Understanding Subversion of Rule-based Inference," *arXiv preprint arXiv:2407.00075*, 2024.

Conferences and Journals

1. X. Ji, A. Xue, E. Wong, O. Sokolsky, and I. Lee, "AR-Pro: Anomaly Explanation and Repair with Formal Properties," *Advances in Neural Information Processing Systems*, vol. 37, 2025.
2. A. Xue, R. Alur, and E. Wong, "Stability Guarantees for Feature Attributions with Multiplicative Smoothing," *Advances in Neural Information Processing Systems*, vol. 36, 2024.
3. A. Xue, L. Lindemann, and R. Alur, "Chordal Sparsity for SDP-based Neural Network Verification," *Automatica*, vol. 161, p. 111 487, 2024.
4. C. Zhu, Z. Li, A. Xue, *et al.*, "{TYGR}: Type Inference on Stripped Binaries using Graph Neural Networks," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 4283–4300.
5. A. Xue, L. Lindemann, A. Robey, H. Hassani, G. J. Pappas, and R. Alur, "Chordal Sparsity for Lipschitz Constant Estimation of Deep Neural Networks," in *2022 IEEE 61st Conference on Decision and Control (CDC)*, IEEE, 2022, pp. 3389–3396.

6. R. Alur, P. Hilliard, Z. G. Ives, *et al.*, "Synchronization Schemas," in *Proceedings of the 40th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems*, 2021, pp. 1–18.

7. O. Bastani, S. Li, and A. Xue, "Safe Reinforcement Learning via Statistical Model Predictive Shielding," in *Robotics: Science and Systems*, 2021.

8. K. S. Namjoshi and A. Xue, "A Self-certifying Compilation Framework for Webassembly," in *Verification, Model Checking, and Abstract Interpretation: 22nd International Conference, VMCAI 2021, Copenhagen, Denmark, January 17–19, 2021, Proceedings 22*, Springer, 2021, pp. 127–148.

9. A. Xue and N. Matni, "Data-driven System Level Synthesis," in *Learning for dynamics and control*, PMLR, 2021, pp. 189–200.

10. W. T. Hallahan, A. Xue, M. T. Bland, R. Jhala, and R. Piskac, "Lazy Counterfactual Symbolic Execution," in *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2019, pp. 411–424.

11. W. T. Hallahan, A. Xue, and R. Piskac, "G2Q: Haskell Constraint Solving," in *Proceedings of the 12th ACM SIGPLAN International Symposium on Haskell*, 2019, pp. 44–57.

Work and Internship Experience

2022 ◇ **SRI International**
Summer Research Intern. Manager: Susmit Jha
Designed and implemented sum-of-squares-based convex optimization methods for verifying neural networks.

2019 ◇ **Nokia Bell Labs**
Summer Research Intern. Advisor: Kedar Namjoshi
Developed a self-certifying compiler framework for WebAssembly. Paper accepted at the Conference on Verification, Model Checking, and Abstract Interpretation, 2021.

2018 ◇ **Harvard University School of Engineering and Applied Sciences**
Summer Research Intern. Advisor: Stephen Chong
Formalized execution semantics of the R programming language. Workshop submission accepted at Formal Methods in Computer-Aided Design, 2018.

2017 ◇ **Max Planck Institute for Software Systems**
Summer Research Intern. Advisors: Rupak Majumdar and Damien Zufferey
Applied model-checking to 3D printer firmware and contributed to the dReal SMT solver.

2016 – 2019 ◇ **Yale University Computer Science Department**
Undergraduate Research Assistant. Advisor: Ruzica Piskac
Developed a symbolic execution engine for Haskell. Paper submission accepted at Programming Language Design and Implementation, 2019.

2014 – 2015 ◇ **Harvard Medical School**
Software Engineering Intern. Advisor: Nils Gehlenborg
Developed visualization software with D3 and contributed to the refinery platform for web-based data visualization.

2014 ◇ **Vertex Pharmaceuticals**
Summer Software Engineering Intern. Manager: Jason Yuen
Developed an inventory scanner and manager for iOS.

2013 ◇ **Vertex Pharmaceuticals**
Summer Software Engineering Intern. Manager: Jason Yuen
Developed bug-tracking database using Google Web Toolkit.

Teaching Experience

Spring 2023 ◇ **Convex Optimization**
UPenn ESE 605, TA

2020 – 2021 ◇ **Fundamentals of Linear Algebra and Optimization**
UPenn CIS 515, TA, Fall 2020, Spring 2021

Summer 2020 ◇ **Mathematical Foundations of Computer Science**
UPenn CIS 160, TA

Spring 2019 ◇ **Real Analysis**
Yale MATH 305, Course Grader

Spring 2018 ◇ **Intensive Algorithms**
Yale CPSC 366, TA

Spring 2017 ◇ **Design and Analysis of Algorithms**
Yale CPSC 365, TA

2016 – 2018 ◇ **Mathematical Tools for Computer Science**
Yale CPSC 202, TA, Fall 2016, Fall 2017, Fall 2018

Projects Supervised

2023 – ◇ **Faraz Rahman** (UPenn Undergraduate)
Topic: Explainability and Interpretability of Diffusion Models

2023 – ◇ **David Zhang** (UPenn Undergraduate)
Topic: Adversarial Robustness of In-context Learning

2023 ◇ **Jawad Ahmad** (Friends Select School, Philadelphia)
Topic: Programmer-friendly Code Synthesis with Chat-GPT.

Research Community Service

2024 – ◇ **NeurIPS, ICLR**
Reviewer

2023 – ◇ **SATA, SciForDL, AdvML**
Reviewer

2021 – ◇ **IEEE L-CSS, CDC, ACC, Automatica, L4DC**
Reviewer

2023 ◇ **Tools and Algorithms for the Construction and Analysis of Systems**
Artifact Evaluation Committee

2022 ◇ **Principles of Programming Languages**
Student Volunteer

2021 ◇ **Static Analysis Symposium**
Artifact Evaluation Committee

2021 ◇ **Conference on Verification, Model Checking, and Abstract Interpretation**
Artifact Evaluation Committee

2019 – 2021 ◇ **Programming Language Design and Implementation**
Student Volunteer (2019), Artifact Evaluation Committee (2020, 2021)

2017, 2019 ◇ **Computer Aided Verification**
Student Volunteer

2017 – 2018 ◇ **Yale University Computer Science Department**
Department Student Advisory Committee