Matthew Yacavone

yacavone.net | matthew@yacavone.net | github.com/m-yac
Brooklyn, NY | +1 973 330 6645

Experience

Software Engineer / Researcher

2020-2024 | Galois, Inc.

Created, developed, and maintained powerful tools for formal verification.

- Was a core contributor to *SAW (Software Analysis Workbench)*, a large, decade-old suite of formal verification tools in active use as part of critical systems in US government and commercial clients.
  - Spearheaded the design, interface, and development of *Mr. Solver,* a tool within *SAW* for automatically proving the correctness of a large class of programs which *SAW* previously couldn't handle: unbounded programs – i.e. those with variable or infinite length loops.
  - Primarily designed, implemented, and maintained *Coq* automation for *Heapster*, a tool within *SAW* for analyzing unbounded programs – the output of which being what *Mr. Solver* is designed to work with.
  - Co-authored two papers (publications [1], [3]) on *Heapster*, both of which use and rely on my automation for their core results.
  - Verified, with a colleague, the correctness of a software update mechanism developed for a DoD client using *Heapster's Coq* automation. Verified the top-level interface of Dilithum, a NIST-standard post-quantum signature scheme, using *Mr. Solver*.
- Audited a large Python codebase implementing Differential Privacy for a government client, resulting in authoring and delivering a 21-page document analyzing the mathematical probability of two key sampling routines failing via integer overflow. Updated their codebase to precisely predict and account for these overflows.

Research in Knot Theory

2019-2022 | Haverford College

Developed and proved a novel result in Legendrian Knot Theory in collaboration with my former professor Joshua Sabloff. Co-authored and published a paper in a major knot theory journal (publication [2]).

- Created an interactive user interface in Python for experimenting with and collecting data on Legendrian knots, used to develop our result.

Education

B.S. Mathematics from Haverford College, 2019

Included two semesters of graduate studies in mathematics at the University of Pennsylvania.

Skills

Interactive Web Design

Four years of experience creating interactive tools/visualizations for music theory, linguistics, and more – all available on my website.

Programming Languages/Libraries

- *Web:* HTML, CSS, Javascript, Typescript, Node, Jekyll
- *Data:* Python, SciPy, Matplotlib
- *Verification:* Haskell, Agda, Coq

Publications

[3] Silver, L., Westbrook, E., Yacavone, M., & Scott, R. (2023). **Interaction Tree Specifications: A Framework for Specifying Recursive, Effectful Computations That Supports Auto-Active Verification.** In *37th European Conference on Object-Oriented Programming (ECOOP 2023)*. [PDF]

[2] Guadagni, R., Sabloff, J. M., & Yacavone, M. (2022). **Legendrian satellites and decomposable cobordisms.** *Journal of Knot Theory and Its Ramifications, 31* (13), Article 2250071. [PDF]

[1] He, P., Westbrook, E., Carmer, B., Phifer, C., Robert, V., Smeltzer, K., Ștefănescu, A., Tomb, A., Yacavone, M., & Zdancewic, S. (2021). **A type system for extracting functional specifications from memory-safe imperative programs.** *Proceedings of the ACM on Programming Languages, 5 (OOPSLA)*, Article 135, 1-29. [PDF]