TEMPLE UNIVERSITY®

Temple University
Computer and Information Sciences

Verification for Every-day Programming

Jay McCarthy
Vassar College

Friday, March 20, 11AM, SERC 306

Abstract:
Most programmers associate formal verification and mechanical theorem proving with formalizing mathematics, high assurance software (such as aerospace control systems), and hardware checking, but not their own work. Yet, recently these approaches have found success in more commonplace applications such as C compilers and relational databases. We attribute this expansion to a greater appreciation of reliable software and a decrease in the cost of verification.

In this talk, I will describe my own forays into this area with an emphasis on how formal verification creates practical benefits that would not have been available if not for the reliability of the theorems. I have selected a diverse set of applications for this presentation:

- how random testing of programs can be improved with formally verified fair enumeration of input data;
- how traditional network services, like load-balancers, must adapt to handle the unique constraints of cryptographic protocols;
- how simple probabilistic relationships need a foundation in complex measure theory to understand and automate;
- how modern APIs assume users obey temporal orderings in their uses which need a new kind of monitoring system to enforce at runtime.

Finally, I will close with a sketch of further ways that this application of programming language and verification research can improve software quality and programmer quality of life.

Biosketch:

Jay McCarthy is a visiting assistant professor at Vassar College and was an assistant professor at Brigham Young University, both in the Computer Science Department. He is a member of the PLT research group and works on the Racket programming language. He completed a PhD at Brown University in the Computer Science Department under Shriram Krishnamurthi as an NSF Graduate Research Fellow. He did his BS at the University of Massachusetts at Lowell studying Mathematics, Computer Science, and Economics. He is passionate about computer science education & diversity, formal verification, programming language expressiveness, and his three adorable kids.