TALKS @ LASIGE driven by excellence

Fri 11 November 2022

GRADUAL VERIFICATION: ASSURING SOFTWARE INCREMENTALLY

Speaker

Jonathan Aldrich

Affiliation

Carnegie Mellon University

When

November 11, 15h

Where

FCUL, room 6.3.27

Abstract

Current static verification techniques do not provide good support for incrementality, making it difficult for developers to focus on specifying and verifying the properties and components that are most important. Dynamic verification approaches support incrementality, but cannot provide static guarantees. To bridge this gap, we propose gradual verification, which supports incrementality by allowing every assertion to be complete, partial, or omitted, and provides sound verification that smoothly scales from dynamic to static checking. I'll describe a system that can verify first-order specifications of programs that manipulate recursive, mutable data structures on the heap, demonstrate a prototype tool, and share some initial empirical results. Our approach addresses several technical challenges, such as semantically connecting iso- and equi-recursive interpretations of abstract predicates, and supporting gradual verification of heap ownership. This work thus lays the foundation for future tools that work on realistic programs and support verification within an engineering process in which cost-benefit tradeoffs can be made.

Bio

Jonathan Aldrich is a Professor of Computer Science at Carnegie Mellon University. He teaches courses in programming languages, software engineering, object-oriented design, and program analysis for quality and security. Prof. Aldrich directed CMU's Software Engineering Ph.D. program from 2013-2019.

Dr. Aldrich's research centers on programming languages and type systems that are deeply informed by software engineering considerations. His research contributions include modular and gradual verification of functional properties, typestate, and architectural structure, as well as the design of languages and type systems for usability. His notable awards include an NSF CAREER award (2006), the Dahl-Nygaard Junior Prize (2007), the DARPA Computer Science Study Group, and an ICSE most influential paper award (2012). He served as general chair (2015), program chair (2017), and steering committee chair (2017-2019) of SPLASH and OOPSLA. Aldrich holds a bachelor's degree in Computer Science from Caltech and a Ph.D. from the University of Washington.