CS Talk Series

Turning Iris Up to Eleven: Next Steps in Higher-Order Separation Logic

Derek Dreyer
MPI-SWS

Host: Thomas Henzinger

Iris is a framework for higher-order concurrent separation logic, implemented in the Coq proof assistant, which we have been developing since 2014. Originally designed for pedagogical purposes, Iris has grown into a ongoing, multi-institution project, with active collaborators at Aarhus University, BedRock Systems, Boston College, CNRS/LRI, Groningen University, INRIA, ITU Copenhagen, KU Leuven, Microsoft Research, MIT, MPI-SWS, NYU, Radboud University Nijmegen, Saarland University, and Vrije Universiteit Brussel, and over 35 published papers studying or deploying Iris for verification of complex programs and programming language meta-theory in Rust, Go, OCaml, Scala, and more (https://iris-project.org). In this talk, we will present two brand new -- and very different -- developments that have the potential to extend the reach of Iris even further. The first is a new *ownership-based refinement type system* for C, which supports *automated* verification of C programs while at the same time being *foundational* (producing Iris proofs in Coq).The second is a complete "remodeling" of Iris, replacing its original step-indexed model with a *transfinite* step-indexed model in order to make Iris suitable for verification of liveness properties. For this talk, we will not assume any prior knowledge of Iris.Rather, we will briefly review the distinguishing features of Iris, and then explain the key insights behind the aforementioned new developments -- and the problems they are solving -- at a high level of abstraction. The first new development is joint work with Michael Sammler, Rodolphe Lepigre, Robbert Krebbers, Kayvan Memarian, and Deepak Garg. The second is joint work with Simon Spies, Lennard Gäher, Daniel Gratzer, Joseph Tassarotti, Robbert Krebbers, and Lars Birkedal. Speaker Bio: Derek Dreyer is a tenured faculty member of the Max Planck Institute for Software Systems (MPI-SWS) in Kaiserslautern and Saarbrücken, Germany, where he leads the “Foundations of Programming” group. He also leads the RustBelt project, funded by an ERC Consolidator Grant, which investigates the formal properties of Rust, a new major systems programming language, in close collaboration with its developers at Mozilla. Derek was awarded the ACM SIGPLAN Robin Milner Young Researcher award in 2017, and, also in 2017, distinguished paper awards at each of OOPSLA, ECOOP, and PLDI.

Monday, December 14, 2020 02:00pm - 03:00pm

Zoom Link:

https://istaustria.zoom.us/j/98682447989?pwd=ZThFV1hYMXBpQ2FzVmxUbnVldS9VZz09
(Meeting ID: 986 8244 7989 | Passcode: 192229)

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station.
Please find a schedule of the ISTA Shuttle on our webpage:
https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.