Interactive and Automated Proofs in Modal Separation Logic

Robbert Krebbers
Radboud University, Nijmegen, The Netherlands

Abstract

In program verification, it is common to embed a high-level object logic into the meta logic of a proof assistant to hide low-level aspects of the verification. To verify imperative and concurrent programs, separation logic hides explicit reasoning about heaps and pointer disjointness. To verify programs with cyclic features such as modules or higher-order state, modal logic provides modalities to hide explicit reasoning about step-indices that are used to stratify recursion.

The meta logic of proof assistants such as Coq is well suited to embed high-level object logics and prove their soundness. However, proof assistants such as Coq do not have native infrastructure to facilitate proofs in embedded logics – their proof contexts and built-in tactics for interactive and automated proofs are tailored to the connectives of the meta logic, and do not extend to those of the object logic. This results in proofs that are at a too low level of abstraction because they are cluttered with bookkeeping code related to manipulating the object logic.

In this talk I will describe our work in the Iris project to address this problem – first for interactive proofs, and then for semi-automated proofs. The *Iris Proof Mode* provides high-level tactics for interactive proofs in higher-order concurrent separation logic with modalities. Recent work on *RefinedC* and *Diaframe* have built on top of the Iris Proof Mode to obtain proof automation for low-level C programs and fine-grained concurrent programs.

2012 ACM Subject Classification Theory of computation → Separation logic; Theory of computation → Automated reasoning; Theory of computation → Program verification

Keywords and phrases Program Verification, Separation Logic, Step-Indexing, Modal Logic, Interactive Theorem Proving, Proof Automation, Iris, Coq

Digital Object Identifier 10.4230/LIPIcs.ITP.2023.2

Category Invited Talk

Acknowledgements I thank my coauthors of the Iris Proof Mode (POPL'17, ICFP'18), RefinedC (PLDI'21), and Diaframe (PLDI'22, PLDI'23, OOPSLA'23) papers: Lars Birkedal, Arthur Charguéraud, Łukasz Czajka, Derek Dreyer, Deepak Garg, Herman Geuvers, Jacques-Henri Jourdan, Ralf Jung, Jan-Oliver Kaiser, Rodolphe Lepigre, Kayvan Memarian, Ike Mulder, Michael Sammler, Joseph Tassarotti, and Amin Timany. I thank all contributors to the Iris project.