Fully Compositional Inductive Invariant Inference in TLA+

Ian Dardik, Ph.D. Student, Carnegie Mellon University
Eunsuk Kang, Associate Professor, Carnegie Mellon University

Online talk by Ian Dardik (left)

Hosted by the TLA+ Foundation

September 30, 2025 @ 11am EST

Zoom link:
https://zoom-lfx.platform.linuxfoundation.org/meeting/92502192791?password=d1d3b88a-d8d1-4337-869e-2c50c6944df2

Abstract

A key advantage to formal methods, such as TLA+, is the ability to *verify* that a specification is correct with respect to its desired properties. While the TLC model checker can show correctness for finite instances of a specification, it is often necessary to find an *inductive invariant* to prove that the specification is correct for all possible instances.

Inductive invariants are logical formulas that are notoriously complex and hard to create manually. As a result, the problem of automated *inductive invariant inference* is an active research topic. Despite recent progress in this area, complex specifications, such as Raft, currently remain out of reach for the state-of-the-art invariant inference tools.

In this research project, we propose *fully compositional* inductive invariant inference with the goal of extending invariant inference to complex, real-world specifications. Our main innovation is the first divide-and-conquer framework for invariant inference. Our framework verifies a TLA+ specification in the following four steps: (1) Decomposition: decompose the specification into smaller components, (2) Contract Creation: create an *assume-guarantee contract* for each component, (3) Local Inference: infer a *local inductive invariant* to prove each component's contract, and (4) Global Correctness: by construction, the conjunction of all local invariants is an inductive invariant *for the entire system.*

Additionally, we present an algorithm for synthesizing assume-guarantee contracts for TLA+ components, which can be used to automate step (2) of our framework. We have implemented the algorithm in a research prototype tool called Carini, which is publicly available for use by the TLA+ community.

We showcase our fully compositional invariant inference framework by using it to verify several specifications, including a specification of Raft used at MongoDB. We view these encouraging results as a call for future research into compositional inductive invariant inference.

This research project is funded by a grant from the TLA+ Foundation
https://foundation.tlapl.us/

S3D Software and Societal Systems Department
Carnegie Mellon University School of Computer Science