Invited Talk: Deductive Verification of Distributed Protocols in Decidable Logics

Oded Padon[1]

[1]VMware Research

Abstract

Verification of distributed protocols and systems, where both the number of nodes in the systems and the state-space of each node are unbounded, is a long-standing research goal. In recent years, efforts around the Ivy verification tool have pushed a strategy of modeling distributed protocols and systems in a new way that enables decidable deductive verification, i.e., given a candidate inductive invariant, it is possible to automatically check if it is inductive, and to produce a finite counterexample to induction in case it is not inductive. Complex protocols require quantifiers in both models and their invariants, including forall-exists quantifier alternations. Still, it is possible to obtain decidability by enforcing a stratification structure on quantifier alternations, often achieved using modular decomposition techniques. Stratified quantifiers lead not only to theoretical decidability, but to reliable solver performance in practice, which is in contrast to the typical instability of SMT solvers over formulas with complex quantification. Moreover, reliable automation of invariant checking and finite counterexamples open the path to automating invariant inference. Recently, several invariant inference algorithms have been developed that can find complex quantified invariants for challenging distributed protocols. In this talk I will provide an overview of Ivy's principles and techniques for modeling distributed protocols in a decidable fragment of first-order logic. I will also draw on the experience with Ivy and related tools to offer some lessons learned and open questions relevant to the SMT community.

SMT'23: 21st International Workshop on Satisfiability Modulo Theories, July 5–6, 2023, Rome, Italy

oded.padon@gmail.com (O. Padon)