Simple Invariants for Proving the Safety of Distributed Protocols

Mooly Sagiv

Tel Aviv University, Tel Aviv, Israel
mooly.sagiv@gmail.com

Abstract

Safety of a distributed protocol means that the protocol never reaches a bad state, e.g., a state where two nodes become leaders in a leader-election protocol. Proving safety is obviously undecidable since such protocols are run by an unbounded number of nodes, and their safety needs to be established for any number of nodes. I will describe a deductive approach for proving safety, based on the concept of universally quantified inductive invariants – an adaptation of the mathematical concept of induction to the domain of programs. In the deductive approach, the programmer specifies a candidate inductive invariant and the system automatically checks if it is inductive. By restricting the invariants to be universally quantified, this approach can be effectively implemented with a SAT solver.

This is a joint work with Ken McMillan (Microsoft Research), Oded Padon (Tel Aviv University), Aurojit Panda (UC Berkeley), and Sharon Shoham (Tel Aviv University) and was integrated into the IVY system[1]. The work is inspired by Shachar Itzhaky's thesis[2].

1998 ACM Subject Classification D.2.4 Software/Program Verification, Formal Methods

Keywords and phrases Program verification, Distributed protocols, Deductive reasoning

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2016.2

Category Invited Talk

[1] http://microsoft.github.io/ivy/
[2] http://people.csail.mit.edu/shachari

36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016).
Editors: Akash Lal, S. Akshay, Saket Saurabh, and Sandeep Sen; Article No. 2; pp. 2:1–2:1
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany