COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

AMAN GOEL

From Finite to Infinite: Scalable Automatic Verification of Hardware Designs and Distributed Protocols

Wednesday, October 13, 2021
2:00pm - 4:00pm
Virtual
Passcode: 654321
Meeting ID: 924 5033 8330

ABSTRACT: As the world increasingly depends on complex systems to transfer messages, store our data, and control our finances, how can we tell whether the system is correct, secure, and reliable? Common practices continue to employ computation-intensive simulation-based verification and tedious manual verification. Formal verification using model checking provides an automatic way to identify functional errors in human-engineered designs. Our work presents a collection of scalable model checking techniques to automatically verify hardware designs and distributed protocols by incorporating often ignored structural information readily available at the design level.

For hardware designs, we developed equality abstraction, a novel technique that abstracts away unimportant low-level specifics and automatically identifies crucial information using equality relations over source-code level objects, such as branch conditions, operations, etc. Our hardware verifier, called AVR, won the prestigious Hardware Model Checking Competition 2020, outperforming state-of-the-art verifiers with a wide margin, and showed large benefits on a variety of challenging industrial-strength designs and RISC-V cores.

Recognizing the lack of automation in verifying distributed protocols, we developed IC3PO, a new verifier that significantly outperforms the state-of-the-art by taking advantage of three structural features in protocol specifications: a) the spatial regularity over replicas that can be permuted arbitrarily, b) the temporal regularity over ordered ranges, and c) the hierarchical protocol structure. IC3PO was able to prove the safety of the Paxos consensus protocol, presenting the first demonstration of an automatically-inferred inductive invariant for Lamport's original Paxos specification.

Both AVR and IC3PO generate mathematical explanations, called certificates, that can be independently checked to guarantee design correctness. They can also generate counterexamples that help in identifying design bugs before deployment resulting in robustness against malicious attacks and reduction in down-times and loss of revenue.

CHAIR: Prof. Karem Sakallah