Modular Proof of Sequential Consistency

Arvind
Computer Science and Artificial Intelligence Laboratory (CSAIL)
Massachusetts Institute of Technology

We present a new framework for modular verification of hardware designs in the style of the Bluespec language. That is, we formalize the idea of components in a hardware design, with well-defined input and output channels; and we show how to specify and verify components individually. As a demonstration, we verify a fairly realistic implementation of a multicore shared-memory system with two types of components: memory system and processor. Both components include nontrivial optimizations, with the memory system employing an arbitrary hierarchy of cache nodes that communicate with each other concurrently, and with the processor doing speculative execution of many concurrent read operations. Nonetheless, we prove that the combined system implements sequential consistency.

Time permitting we will briefly describe our "Chips with Proofs" project.

Murali Vijayaraghavan*, Adam Chlipala, Arvind, and Nirav Dave, "Modular Deductive Verification of Multiprocessor Hardware Designs", CAV 2015*

Biography: Arvind is the Johnson Professor of Computer Science and Engineering at MIT. Arvind's group, in collaboration with Motorola, built the Monsoon dataflow machines and its associated software in the late eighties. In 2000, Arvind started Sandburst which was sold to Broadcom in 2006. In 2003, Arvind co-founded Bluespec Inc., an EDA company to produce a set of tools for high-level synthesis. In 2001, Dr. R. S. Nikhil and Arvind published the book "Implicit parallel programming in pH". Arvind's current research focus is on enabling rapid development of embedded systems. Arvind is a Fellow of IEEE and ACM, and a member of the National Academy of Engineering and the American Academy of Arts and Sciences.