Decomposing the Proof of Correctness of Pipelined Microprocessors

Ravi Hosabettu[1], Mandayam Srivas[2], Ganesh Gopalakrishnan[1]

[1]Department of Computer Science
University of Utah
Salt Lake City, UT 84112

[2]Computer Science Laboratory
SRI International
Menlo Park, CA 94025

Contact email: hosabett@cs.utah.edu

January 12, 1998

Abstract

We present a systematic approach to *decompose* and *incrementally build* the proof of correctness of pipelined microprocessors. The central idea is to construct the abstraction function using *completion functions*, one per unfinished instruction, each of which specify the effect (on the observables) of completing the instruction. In addition to avoiding term-size and case explosion as could happen for deep and complex pipelines during *flushing* and helping localize errors, our method can also handle stages with iterative loops. The technique is illustrated on pipelined- as well as a superscalar pipelined implementations of a subset of the DLX architecture.

Keywords: Processor verification, Decomposition, Incremental verification
Category: A