A Generic Operational Memory Model Specification Framework for Multithreaded Program Verification

Yue Yang, Ganesh Gopalakrishnan,
and Gary Lindstrom

UUCS-03-015

School of Computing
University of Utah
Salt Lake City, UT 84112 USA

September 2, 2003

Abstract

Given the complicated nature of modern architectural and language level memory model designs, it is vital to have a systematic approach for specifying memory consistency requirements that can support verification and promote understanding. In this paper, we develop a specification methodology that defines a memory model operationally using a generic transition system with integrated model checking capability to enable formal reasoning about program correctness in a multithreaded environment. Based on a simple abstract machine, our system can be configured to define a variety of consistency models in a uniform notation. We then apply this framework as a taxonomy to formalize several well known memory models. We also provide an alternative specification for the Java memory model based on a proposal from Manson and Pugh and demonstrate how to conduct computer aided analysis for Java thread semantics. Finally, we compare this operational approach with axiomatic approaches and discuss a method to convert a memory model definition from one style to the other.