Runtime Model Checking of Multithreaded C/C++ Programs

Yu Yang
Xiaofang Chen
Ganesh Gopalakrishnan
Robert M. Kirby

UUCS-07-008

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

March 20, 2007

Abstract

We present `inspect`, a tool for model checking safety properties of multithreaded C/C++ programs where threads interact through shared variables and synchronization primitives. The given program is mechanically transformed into an instrumented version that yields control to a centralized scheduler around each such interaction. The scheduler first enables an arbitrary execution. It then explores alternative interleavings of the program. It avoids redundancy exploration through dynamic partial order reduction(DPOR) Our initial experience shows that `inspect` is effective in testing and debugging multithreaded C/C++ programs. We are not aware of DPOR having been implemented in such a setting. With `inspect`, we have been able to find many bugs in real applications.