Refactoring SPIN for Safety

Robert Palmer and Ganesh Gopalakrishnan

UUCS-06-001

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

February 14, 2006

Abstract

We show how to refactor SPIN for safety model checking resulting in a compact model checker occupying less than 200 lines of code without appreciable loss of performance while reusing much of SPIN's front-end facilities. In addition to being far easier to understand and being eminently suitable as a basis for extensions by the researcher and developer community, the resulting model checker is also eminently suitable for distributed model checking—a project that is underway. We also show that employing graphical means of visualizing the asynchronous product graph can be very valuable in debugging a model checker—a facility we implemented and extensively employed in both understanding the original SPIN and discovering three subtle flaws in it.