

Model Checking Concurrent Programs

Aarti Gupta

NEC Laboratories America, Princeton
agupta@nec-labs.com

Abstract. With the growth of multi-core processing and concurrent programming in modern computing systems, there is a great need to develop effective verification techniques for concurrent programs. Static analysis techniques have been shown effective for finding data races, but suffer from a general problem of too many false alarms. Dynamic techniques like testing have also shown promise, but provide limited coverage over the state space including all possible thread interleavings. Model checking alone cannot scale. However, it works better in combination with these techniques, with the potential of finding real error traces on one hand and better coverage on the other. In this talk, I will describe our recent advances in concurrent dataflow analysis, symbolic model checking with partial order reduction, and dynamic techniques for verifying concurrent programs. These techniques have been implemented in a unified verification platform, currently targeted at multi-threaded C programs. I will also report on our experiences on some challenging examples from the public domain and the industry.