An Interface Aware Guided Search Method for Error-trace Justification in Large Protocols

Xiaofang Chen, Yu Yang and Ganesh Gopalakrishnan

UUCS-08-005

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

Abstract

Many complex concurrent protocols that cannot be formally verified due to state explosion can often be formally verified by initially creating a collection of abstractions (overapproximations), and subsequently refining the overapproximated protocol in response to spurious counterexample traces. Such an approach crucially depends on the ability to check whether a given error trace in the abstract protocol corresponds to a concrete trace in the original protocol. Unfortunately, this checking step alone can be as as hard verifying the original protocol directly without abstractions, which is infeasible. Our approach tracks the *interface behavior* at the interfaces erected by our abstractions, and employs a few heuristic search methods based on a classification of the abstract system generating these traces. This collection of heuristic search methods form a tailor-made guided search strategy that works very efficiently in practice on three realistic multicore hierarchical cache coherence protocols. It could correctly analyze 99 spurious error traces and 3 genuine error scenarios, each within 15 seconds. Also, on 94 of the 99 of the spurious errors, our approach can precisely report which transition in the abstract protocol is overly approximated that leads to the spurious error.