A Dual-Engine for Early Analysis of Critical Systems

Aboubakr Achraf El Ghazi, Ulrich Geilmann, Mattias Ulbrich, Mana Taghdiri

Karlsruhe Institute of Technology, Germany
{elghazi, geilmann, mulbrich, taghdiri}@ira.uka.de

Abstract: This paper presents a framework for modeling, simulating, and checking properties of critical systems based on the Alloy language – a declarative, first-order, relational logic with a built-in transitive closure operator. The paper introduces a new dual-analysis engine that is capable of providing both *counterexamples* and *proofs*. Counterexamples are found fully automatically using an SMT solver, which provides a better support for numerical expressions than the existing Alloy Analyzer. Proofs, however, cannot always be found automatically since the Alloy language is undecidable. Our engine offers an economical approach by first trying to prove properties using a fully-automatic, SMT-based analysis, and switches to an interactive theorem prover only if the first attempt fails. This paper also reports on applying our framework to Microsoft's COM standard and the mark-and-sweep garbage collection algorithm.