Efficient Software Model Checking with Block-Abstraction Memoization

Karlheinz Friedberger
karlheinz.friedberger@ifi.lmu.de
Supervisors: Dirk Beyer
Collaborators: Daniel Baier (CONVEY)

Block-Abstraction Memoization (BAM)

BAM applies a divide-and-conquer strategy for analyzing programs, splitting them into smaller blocks that are then analyzed. We extended the approach for an interprocedural analysis and for a multi-threaded approach. BAM works on a domain-independent level and has a low overhead.

Interprocedural BAM

Supports the analysis of recursive programs

Multithreaded BAM

Distributes workload on several independent threads

JAVA SMT 3 [1]

- Common Java API for SMT solvers
- Supports most used SMT theories
- Provides the most common API features
- 8 SMT solvers
- Typesafe
- Used in several software projects, including CPACHECKER

We evaluated all SMT solvers available in JAVA SMT using several software verification techniques against the same set of tasks, using the same hardware. The results support our claim that each solver has its own fingerprint of features and results.

References