Search Enhancements for Java PathFinder

Igor Andjelkovic, Mirko Stojmenovic, University of Belgrade, Serbia

ADVISOR: Darko Marinov

Background

- Java PathFinder (JPF) is an explicit-state model checker for Java programs
  - Used to find bugs in programs or verify properties
- Backtrackable Java Virtual Machine (JVM)
  - Runs on the top of the host JVM
- Implements different search algorithms for state space exploration
- First open-source tool released by NASA
  - http://javapathfinder.sourceforge.net/

Iterative Context Bounding

- New implementation of a search algorithm for JPF
- Reveals bugs in multithreaded programs using minimal number of preemptions
- Incrementally increases the number of preemptions up to a given bound

Context Bounding Heuristic

- Reduces the state space by bounding the number of preemptive thread switches
- Works with any search algorithm
- Prunes all states that exceed the given bound

Basic Block Coverage Heuristic

- Uses basic block coverage as a heuristic
- Collects information about coverage with one search and uses it with another
- Chooses states from which more coverage will be achieved

Goals and Summary

- Find bugs faster or find more bugs by reordering/pruning the search to reduce
  - State-space explosion
  - Search time
  - Memory requirements
- Developed three search enhancements
  - Iterative context bounding search algorithm
  - Context bounding heuristic
  - Basic block coverage heuristic

Results

- Iterative context bounding
  - Reduces the number of explored states
- Context bounding heuristic
  - Works with any search algorithm
  - Reduces the number of explored states
- Basic block coverage heuristic
  - Explores states with greatest coverage first, thus has a greater chance of finding bug faster
  - Finds bugs up to 90% faster in the second search

Fundamental Questions/Challenges

- How to know what to explore? (What states are “interesting”?)
- What about the unexplored states?
- When there are many code changes between two searches, is the collected coverage information relevant?

Related Work/Interaction with Other Projects

- S. Lauterburg, A. Sobeih, D. Marinov, and M. Viswanathan. Incremental state-space exploration for programs with dynamically allocated data. ICSE 2008
- M. Musuvathi, S. Qadeer. Iterative context bounding for systematic testing of multithreaded programs. PLDI 2007