DIVINE: Explicit-State LTL Model Checker

Vladimír Štill Petr Ročkai Jiří Barnat

Masaryk University

Brno, Czech Republic

7th April 2016

- explicit-state model checking of parallel programs
- using LLVM as an intermediate language
- standard C, C++, and `pthread` libraries nearly completely supported
- exact verification, no bounding, all meaningful interleavings
- supports all language features (including exceptions)
- supports relaxed memory models
- no symbolic data support (yet)

Verification Properties

- assertion safety
- memory safety
- memory leaks
- mutex safety
- uninitialized memory use
- LTL
- gives a counterexample if the property does not hold

Powerful Reduction Techniques

- state space size reduction ($\tau+$ reduction)
  - omission of uninteresting interleavings
- memory footprint reduction (lossless compression)
- parallel and distributed search

DIVINE: Summary

- a powerful explicit-state model checker for C++ programs
- specializes on unit tests of real-world parallel programs
- verifies a variety of properties
- 951 points out of 1240 in the concurrency category
- `https://divine.fi.muni.cz`

DIVINE: Summary

- a powerful explicit-state model checker for C++ programs
- specializes on unit tests of real-world parallel programs
- verifies a variety of properties
- 951 points out of 1240 in the concurrency category
- `https://divine.fi.muni.cz`

Thank you!