CADP 2006: A Toolbox for the Construction and Analysis of Distributed Processes

H. Garavel - F. Lang - R. Mateescu - W. Serwe

INRIA – VASY team

http://www.inrialpes.fr/vasy

What is CADP?

A toolbox for verifying asynchronous systems

- At the crossroads between 2 branches of computer science:
  - Concurrency theory
  - Computer-aided verification
- Development started in 1986 …
  - Caesar: LOTOS compiler / state space generator
  - Aldebaran: bisimulation tool

  … continuously enhanced for 20 years

CADP wrt other model checkers

- Parallel programs (rather than sequential programs)
- Message passing (rather than shared memory)
- Languages with a formal semantics (process calculi)
- Dynamic data structures (records, lists, trees…)
- Explicit-state (rather than symbolic)
- Action-based (rather than state-based)
- Branching-time logic (rather than linear-time logic)

CADP verification features

- Several paradigms:
  - Model checking (modal μ-calculus)
  - Equivalence checking (bisimulations)
  - Visual checking (graph drawing)
- Several techniques:
  - Reachability analysis
  - On-the-fly verification
  - Compositional verification
  - Distributed verification
  - Static analysis

Other CADP features

- Beyond mere verification:
  - Multiple input languages
  - Step-by-step simulation
  - Rapid prototyping
  - Test generation
  - Performance evaluation

- Generic software components for verification
- Modular, extensible architecture (APIs)

The new version CADP 2006

- 5 years of work since CADP 2001
  - 70 successive beta-versions
  - 245 enhancements
  - 150 bug fixes

- New version CADP 2006 "Edinburgh"
  - 42 tools
  - 17 software libraries

(*) *dedicated to the Laboratory for Foundations of Computer Science at the University of Edinburgh for their achievements in concurrency theory (especially their inspiring Concurrency Workbench)*

CADP 2006: 15 new tools

- Explicit state space generation
  - CAESAR 7.0, CAESAR.BDD
- Compositional verification
  - BCG_GRAPH, EXP.OPEN 2.0, PROJECTOR 2.0
- On-the-fly verification
  - CAESAR_SOLVE, BISIMULATOR, EVALUATOR 3.5, REDUCTOR 5.0
- Distributed verification
  - BCG_MERGE, DISTRIBUTOR
- Performance evaluation
  - BCG_STEADY, BCG_TRANSIENT, DETERMINATOR
- Trace-based verification
  - SEQ.OPEN

Emphasis on software quality

- Goal: robust (industrial strength) tools
- Provisions:
  - Mastered development process
  - Controlled evolutions (peer reviewing)
  - Care for backward compatibility
  - Intensive testing
  - Precise documentation

Some figures about CADP 2006

- 4 computing platforms supported
  - Sparc/Solaris, PC/Linux, PC/Windows, MacOS X

- International dissemination
  - License agreements signed with 372 organizations
  - Licenses granted for 822 machines in 2006
  - 94 case-studies accomplished using CADP
  - 29 research tools connected to CADP
  - 28 university lectures based on CADP (since 2002)

Conclusion

- A new toolbox CADP 2006 is available
- 3 targeted application domains:
  - Avionics (Airbus, topcased.org)
  - Multiprocessor architectures (Bull, CEA/Leti, ST)
  - Bioinformatics
- Successful applications: *crucial parts of Tera10 (France's most powerful supercomputer) were verified using CADP*
- Further work is going on (CADP 2007)

For more information…

- CADP demo at CAV 2007
- CADP Web site:
  www.inrialpes.fr/vasy/cadp
- CADP Newsletter #6 (April 2007):
  www.inrialpes.fr/vasy/cadp/news6.html