FM Group's Contributions

P.Camurati G.Cabodi S.Nocco S.Quer

Formal Methods Group
Department of Computer Engineering
Politecnico di Torino
Torino, Italy

Outline

- Politecnico di Torino Reachability Analysis and Verification (PdTRAV)
- Hardware Model Checking Competition (HWMCC)

Outline

- Politecnico di Torino Reachability Analysis and Verification (PdTRAV)
- Hardware Model Checking Competition (HWMCC)

PdTRAV (1/3)

- Politecnico di Torino Reachabity Analysis & Verification (PdTRAV)
  - Prototype academic tool for development and benchmarking of advanced model and equivalence checking algorithms
  - The tool is being (and will be) tested through publicly available as well as industrial problems
  - Made available to SRC industries
- New MC algorithms for industrial problems addressed

PdTRAV (2/3)

- Includes several formal verification engines
- NOT a complete design/verification tool/chain
- Set of algorithms/engines oriented to evaulation/benchmarking

PdTRAV (3/3)

- Bit-level Symbolic Formal Verification
  - Bounded Model Checking
  - Unbounded Model Checking
- Core Techniques/Engines
  - Equivalence checking
  - Reachability with Binary Decision Diagrams (BDDs)
  - Bounded Model Checking (BMC) with SATisfiability (SAT)
  - Abstraction techniques (e.g., localization, CEGAR)
  - Induction-based Unbounded Model Checking
  - Interpolation-based Unbounded Model Checking
  - Property Driven Reachability (IC3)
  - ...

Outline

- Politecnico di Torino Reachability Analysis and Verification (PdTRAV)
- Hardware Model Checking Competition (HWMCC)

Hardware Model Checking Competition

- Revive interest in improving symbolic model checking technology
  - Symbolic model checking does not scale enough
  - Academic research kind of stalled
  - Benchmarks were lacking
- Repeat success story of the SAT competition
  - Simple standardized input format
  - Motivation for young researchers
  - Competition benchmarks used in publications

HWMCC: History

- 1st HWMCC
  - CAV 2007, Berlin
  - Biere, Cimatti, Claessen, McMillan, Somenzi
- 2nd HWMCC
  - CAV 2008, Princeton
  - Biere, Cimatti, Claessen, Jussila, McMillan, Somenzi
- 3rd HWMCC
  - CAV 2010, Edimburgh
  - Biere, Claessen

HWMCC: Benchmarks

- 1st HWMCC
  - 344 benchmarks
  - 4 suites: 175 L2S, 118 TIP, 42 Intel, 9 AMBA
- 2nd HWMCC
  - 344 old, 301 new, 645 total
  - New: 18 Intel, 35 B. Jobstmann, 207 VIS/PdT, 28 PdT, 13 NEC
- 3rd HWMCC
  - 645 old, 173 new, 818 total
  - New: 14 PicoJava 2, 96 Bob Brayton, 48 PdT, 15 Mentor Graphics

HWMCC: Model Checkers (1/2)

- 2007
  - 19 model checkers
  - 3 JKU Litz, 2 ETH Zurich, 2 IRST Trento, 4 PdT, 2 CMU Pittsburg, 1 Cadence Berkeley, 1 Chalmers Cotheburg, 4 CU-Boulder
- 2008
  - 16 model checkers, 2 old, 14 new
- 2010
  - 21 model checkers

HWMCC: Model Checkers (2/2)

- ABC: Bob Brayton's group (Berkeley), 4 variants
- BIP: Niklas E´en (Berkeley)
- CIP + MBMC Stefan Kupferschmid (Freiburg)
- IC3 Aaron Bradley (Boulder) based on inductive clauses
- MCSTI by Anders Franz´en (Sweden)
- TIP Niklas S¨orensson (Sweden), 3 variants
- PDTRAV Torino (Cabodi, Nocco, Quer)
- Old checkers: AigTrav + McAiger from JKU, NuSMV from Trento

HWMCC: Setup

- Single safety property benchmarks
  - One output serves as "bad state detector"
  - Bad state *reachable* ⇒ instance *satisfiable*
  - Bad state *unreachable* ⇒ instance *unsatisfiable*
- AIGER format (http://fmv.jku.at/aiger)
  - AIGER = And-Inverter-Graphs (AIGs) with latches
  - All submitted solvers can read AIGER now except NuSMV
- 900 seconds time limit, 7 GB memory limit

HWMCC: Winners (1/3)

- 1st HWMCC
  - SAT: 1 - nusmv (193), 2 - tip/vis (183), 3 - aiger (182)
  - UNSAT: 1/4 - PdTrav (83, 83, 79, 78), 5 vis (75), 6 smv-cadence (73)
  - SAT+UNSAT: 1/2 pdtrav (251, 248), 3 vis (236), 4 tip (222)

HWMCC: Winners (2/3)

- 2nd HWMCC
  - SAT: 1 - tipbmc (247), 2 - mcaigerbmc (243), 3 - nusmcbmc/pdtravbmc (239)
  - UNSAT: 1 - abc (314), 2 - tipids (307), 3 - tipidi (303), 4 - pdtravitp (302)
  - SAT+UNSAT: 1 - abc (552), 2 - tipind (522), 3 - pdtravitp (517)

HWMCC: Winners (3/3)

- 3rd HWMCC
  - SAT: 1 - abcbmc2 (325), 2 - tipbmc (325), 3 - cip (325)
  - UNSAT: 1 - pdtrav (423), 2 - absuperprove (412), 3 ic3 (405)
  - SAT+UNSAT: 1 – abcsuperprove (732), 2 - pdtrav (731), 3 - ic3 (713)

PdTRAV Recent Results