Model Checking

Kim Guldstrand Larsen
BRICS Machine
Basic Research in Computer Science, 1993-2006

33+45+40 Millkr

100

100

Aalborg

Aarhus

Tools

Other relevant projects
ARTIST, AMETIST
Informationsteknologi
Tools and BRICS

Logic
- Temporal Logic
- Modal Logic
- MSOL

Algorithmic
- (Timed) Automata Theory
- Graph Theory
- BDDs
- Polyhedra Manipulation

Semantics
- Concurrency Theory
- Abstract Interpretation
- Compositionality
- Models for real-time & hybrid systems

Applications

visualSTATE
- PVS

SPIN
- HOL

UPPAAL
- TLP
- ALF

Applications

Tools and BRICS
CISS: Center for Embedded Software Systems

Kim Guldstrand Larsen
kgl@cs.auc.dk
96358893

or

www.ciss.dk
info@ciss.dk
96357220

Aalborg Universitet
Fr. Bajersvej 7B
9220 Aalborg Ø
Why CISS?

- 80% of all software is embedded
- Demands for increased functionality with minimal resources
- Requires multitude of skills
  - Software construction
  - Hardware platforms,
  - Communication
  - Testing & verification

Goal:
Give a qualitative lift to current industrial practice !!!!!
CISS in Numbers

- Jutland-Fun IT-initiative, 2002:
  - 25,5 mil. kr Ministry
  - 6 mil. kr North Jutland
  - 6 mil. kr Aalborg City
  - 12,75 mil. kr Companies
  - 12,75 mil. kr AAU

- 26 projects
- 20 CISS employees
- 25 CISS associated researcher at 3 different research groups at AAU

- 16 industrial PhDs
ARTIST2
European Network of Excellence

6,5MEuro, 32 partners

EU’s 7th Framework
→
ARTEMIS Research Platform
→
Centers of Excellence
Modelling and Checking

**Plant**
- Continuous

**Controller Program**
- Discrete

Model of environment (user-supplied / non-determinism)

Model of tasks (automatic?)

Sensors and actuators:
- Sensors connect the plant to the controller program.
- Actuators connect the controller program back to the plant.
Model Checking

Finite State Systems
Markovian Decision Processes
Timed Automata
Priced Timed Automata

Requirement $F$

Datastructures & Algorithms
BDD, DBM, CDD, MTBDD, ...
Prototypes
Executable Code
Test sequences

Tools: UPPAAL, visualSTATE, PRISM, RAPTURE, SPIN, Statemate, Verilog, Formalcheck,...
**Benefits of Model Checking**

- General Verification approach (hardware, embedded systems, software)
- Support of partial verification.
- Insensitive to likelihood of error (in contrast to testing).
- Provision of diagnostic information
- Push-button technology
- Rapidly increasing interest by industry (in particular hardware and embedded systems).
- Shorten development time.
- Easily integrated in existing development cycle.
- Not too steep learning curve.
- Sound and mathematical underpinning.
Weaknesses of Model Checking

- Mainly appropriate to control-intensive and less to date-intensive applications.
- Limited by decidability issues.
- Verification of system model and not actual system.
- Only check for stated properties.

- Suffers from state-explosion.
- Requires expertise in finding appropriate abstractions and requirements.
- Model checkers may themselves have bugs.
- Verification of instances with specific parameters and no. of components.
‘State Explosion’ Problem

All combinations: exponential in no. of components

Provably theoretical intractable
Overview (Day 1)

- **Finite State Model Checking**
  - Kripke Structures
  - CTL: Computational Tree Logic
  - Explicit Model Checking Algorithms

- **Symbolic Model Checking**
  - Binary Decision Diagrams
  - Symbolic Model Checking of CTL
  - Compositional Backwards Reachability

- **Probabilistic Model Checking**
  - Discrete Time Markov Chains & Decision Processes
  - Probabilistic Reachability
  - Probabilistic CTL
  - Abstraction/Refinement
Overview (Day 2)

- **Real Time Model Checking**
  - Timed Automata
  - Timed CTL

- **Symbolic Real Time Model Checking**
  - Regions and Zones
  - Symbolic Reachability Checking
  - Symbolic Liveness Checking

- **Further Optimizations**
  - Abstractions & Approximate Analyses
  - Modelling Patterns
  - ...

- **Optimal Scheduling using Model Checking**
  - Priced Timed Automata, Priced Zones
  - Optimal Reachability
  - Optimal Safety
Reading Material

- Consult CAV’06: “25 Years of Model Checking”.


Reading Material

- G. Behrmann, A. David, K.G. Larsen: *Tutorial on UPPAAL* (see www.uppaal.com)

- BOOKS:
  - *Model Checking* by Ed Clarke, Orna Grumberg, Doron Peled
  - *Systems and Software Verification* by B. Berard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, P. Schnoebelen
    coming soon at a book-store near you.