T–79.4301 Parallel and Distributed Systems (4 ECTS)

T–79.4301 Rinnakkaiset ja hajautetut järjestelmät (4 op)

Lecture 12

23rd of April 2007

Keijo Heljanko

Keijo.Heljanko@tkk.fi

Model Checking Tools

- In the following slides model checking tools other than Spin are described
- All the tools are freely available (under various licences) unless otherwise stated
- The comments on the strengths of the tools are highly subjective
- See the table of model checkers at: `http://anna.fi.muni.cz/yahoda/`

NuSMV 2

- Homepage: `nusmv.irst.itc.it/`
- A model checker (mainly) for hardware, a remake of the SMV model checker
- BDD based symbolic model checker
- Bounded model checker
- Licence: LGPL

Java Pathfinder 2

- Homepage: `http://javapathfinder.sourceforge.net/`
- A model checker for Java programs
- Implementation technique: A full custom Java virtual machine
- See also other Java model checkers such as Bandera (`http://bandera.projects.cis.ksu.edu/`) and Bogor (`http://bogor.projects.cis.ksu.edu/`).

Uppaal

- Homepage: `http://www.uppaal.com/`
- A model checker for timed systems
- See also other model checkers for timed systems such as: IF (`http://www-verimag.imag.fr/~async/IF/`) which also handles untimed systems

SLAM

- Homepage: `http://research.microsoft.com/slam/`
- A model checker for sequential C programs (correct use of locking primitives in Windows device drivers) heavily employing abstraction
- Licence: Not available outside Microsoft
- See also: Zing (`http://research.microsoft.com/zing/`)

Maria

- Homepage: `http://www.tcs.hut.fi/Software/maria/`
- A model checker for high-level Petri nets
- Good support for LTL model checking under fairness
- Very extensive data manipulation support, quite flexible as a model checker back-end
- Licence: GPL

PROD

- Homepage: `http://www.tcs.hut.fi/Software/prod/`
- A model checker for high-level Petri nets (Pr/T-nets)
- Very good partial order reduction algorithms available (even better than Spin in many cases)

Murφ

- A model checker for asynchronous systems in a formalism closely related to Petri nets
- Good symmetry reduction algorithms available

The Model Checking Kit

- Homepage:

  `http://www.fmi.uni-stuttgart.de/szs/tools/mckit/overview.shtml`
- A collection of different model checking tools behind a single interface
- Provides an easy way to try different methods on small model checking problems

Members of Model Checking Group

- Leader: Academy Research Fellow Keijo Heljanko
- Members:
  - D.Sc. (Tech.) Tommi Junttila, D.Sc. (Tech.) Heikki Tauriainen, M.Sc. (Tech.) Jori Dubrovin
  - In addition a small number of undergrad students
- Alumni: D.Sc. (Tech.) Toni Jussila (University of Linz, Austria), D.Sc. (Tech.) Timo Latvala (Space Systems Finland (SSF)), and D.Sc. (Tech.) Misa Keinänen (SSF).
- Selected as one of three "Outstanding junior research groups of Helsinki University of Technology (TKK)" Aug 2006–Jul 2008

Research Goal

The main goal of the research is to create methods and tools to enable the cost efficient development of correctly functioning software systems. The main methods are:

- Model based software design: The development of methods and tools that enabled software to be model checked early in the design cycle.
- Bounded model checking: An efficient symbolic model checking method employing techniques from computational logic
- Symbolic partial order methods: Creating methods combining the theory of concurrency with symbolic model checking methods

Teaching of Verification

- T–79.4301 Parallel and Distributed Systems, Spring
- T–79.5301 Reactive Systems, Spring
- T–79.5302 Symbolic Model Checking,
  every second year, next time Autumn 2007
- T–79.5303 Safety Critical Systems,
  given by specialist teacher from the industry, Spring
- T–79.5304 Formal Conformance Testing,
  given by specialist teacher from the industry,
  every second year, next time Autumn 2008
- T–79.5305 Formal Methods,
  every second year, next time Autumn 2008