Model Checking Research Group

Keijo Heljanko

Keijo.Heljanko@tkk.fi
The Cost of Software Defects

The national economic impacts of software defects are significant. In the USA the cost of software defects has been estimated to be $59 billion, that is 0.6% of the gross domestic product.

Source: National Institute of Standards & Technology (NIST): The Economic Impacts of Inadequate Infrastructure for Software Testing


According to NIST, 1/3 of the costs could be avoided by using better software development methods.
An Expensive Bug: Pentium FDIV

The floating point division algorithm uses a table of constants with 1066 rows. A bug in the initialization of the table caused only 1061 rows to be correctly initialized.

Cost: $500 million
Ariane 5

Self destructed 37 seconds after takeoff - the cause was an overflow in the conversion from a 64 bit floating point number to a 16 bit integer.

Cost: $500 million
Finding Bugs in Software

The principal methods for the validation of complex software/hardware systems are:

- Testing (using the system itself)
- Simulation (using a model of the system)
- Model Checking (≈ exhaustive testing of all behaviors of a model of the system)

The main research topic of the group is symbolic model checking.
Model Checking in the Industry

- **Microprocessor design**: All major microprocessor manufacturers use model checking methods as a part of their design process.

- **Design of Data-Communications Protocol Software**: Model checkers have been used as rapid prototyping systems for validating new data-communications protocols under standardization.

- **Critical Software**: NASA space program is model checking code used by the space program.

- **Operating Systems**: Microsoft is using model checking to verify the correct functioning of new Windows device drivers.
Dept. of Information and CS

- 9 Professorships, 100+ researchers
- The model checking group is a subgroup of the computational logic group led by Prof. Ilkka Niemelä
Members of Model Checking Group

- Leader: Academy Research Fellow Keijo Heljanko
- Vice leader: D.Sc. (Tech.) Tommi Junnilla
- D.Sc. (Tech.) Heikki Tauriainen
- M.Sc. (Tech.) Jori Dubrovin
- M.Sc. Siert Wieringa
- In addition 9 research assistants (some part time)

- Alumni: D.Sc. (Tech.) Toni Jussila (OneSpin Solutions, Munich, Germany), D.Sc. (Tech.) Misa Keinänen, D.Sc. (Tech.) Timo Latvala (Space Systems Finland)
Strengths of the Group

- Building on a strong research tradition: Verification topics have been researched in the unit since 1980s.
- Multidisciplinary research: The group combines expertise on symbolic model checking, computational logic, and concurrency theory in one group.
- Good supporting environment in the Department: Close co-operation with other members of the computational logic group.
- Strong International contacts
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.
Main Achievements


- A new state-of-the-art approach to bounded model checking, implemented into the NuSMV2 system:
Main Sources of Funding


Main Sources of Funding (cnt.)


International Contacts

Recent international collaborations include:

- TU München: Prof. J. Esparza
- University of Linz: Prof. A. Biere
- FBK IRST, Trento, Italy: Dr. A. Cimatti and his group
- LMU München: Dr. M. Lange
Teaching of Verification

- T–79.4301 Parallel and Distributed Systems
- T–79.5301 Reactive Systems
- T–79.5302 Symbolic Model Checking, every second year
- T–79.5304 Formal Conformance Testing, given by specialist teacher from the industry, every second year
- T–79.5305 Formal Methods, every second year
The main goal of the research is to create methods and tools to enable the cost efficient development of correctly functioning software systems.

A multidisciplinary research group in model checking combining expertise on:
- Symbolic model checking
- Computational logic
- Concurrency theory

Good background organization: Dept. of Information and Computer Science

Strong International contacts