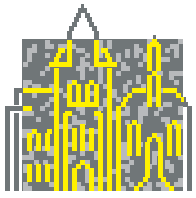
D. Basin (ETH Zürich, CH), H. Ganzinger (MPI Saarbrücken, D), J. Harrison (Intel, US), A. Pnueli (Weizmann Inst., IL)
(Editors)

Applied Deductive Verification

Dagstuhl Seminar 03451 – November 02 to November 07, 2003
Dagstuhl-Seminar-Report No. 401



SCHLOSS DAGSTUHL

INTERNATIONALES
BEGEGNUNGS-
UND FORSCHUNGSZENTRUM
FÜR INFORMATIK

ISSN 0940-1121

Herausgegeben von IBFI gem. GmbH, Schloss Dagstuhl, 66687 Wadern, Germany.

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) Schloss Dagstuhl ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Gesellschafter:

- Gesellschaft für Informatik e.V. – Bonn
- TH Darmstadt
- Universität Frankfurt
- Universität Kaiserslautern
- Universität Karlsruhe
- Universität Stuttgart
- Universität Trier
- Universität des Saarlandes

Summary

Software and hardware systems are increasingly employed in safety or mission critical applications. Deductive verification can be used during development to minimize the risk of their failure. Although the costs associated with verification are often considered high, verification methods have achieved considerable success and there is increasing industrial interest in applying such methods.

The aim of this Dagstuhl seminar was to bring together researchers from academia and industry who are applying deduction to substantial "real-world" problems. We interpret deduction in a broad sense including interactive and automated theorem proving, model checking, program analysis, and the use of decision procedures. Deductive verification is the application of these methods to system analysis; its scope ranges from using theorem provers to carry out full-scale system verification to more light-weight applications that are easier to automate, such as analyzing system properties using model checkers or other decision procedures. Topics relevant for the seminar included research on:

- promising application-oriented foundations,
- method combination (e.g., integrating deduction and model checking), and
- abstraction and other techniques that can reduce the complexity of verification problems.

Applications include:

- Software verification, including protocols, concurrent systems, multimedia applications, and security,
- Hardware verification, including pipelined architectures and cache protocols as well as parameterized verification, and
- Tool verification, i.e., the verification of tools used in safety critical application, such as hardware-targeted compilers.

During the seminar we aimed to achieve a cross-fertilization between theoreticians and practitioners working in the area. This was achieved both by overview talks on the state of the art in the application of deductive methods, and by providing a forum for communication between researchers working on theory with practitioners from industry who are applying verification tools to large-scale applications. The seminar also featured evening tutorials and tool demonstrations.

Scientific Highlights

Formal techniques are increasingly being used to tackle ‘real-world’ industrial applications, and several speakers provided evidence of this. For example, Thomas Arts gave a

fascinating overview of formal verification activity at Ericsson, while Patrick Cousot discussed a rigorous proof that the avionics software used in current Airbus aircraft cannot encounter floating-point overflows.

While we have not yet reached the stage of being able to perform a complete verification of large systems, we have many examples of proving either 'big properties of small systems' or 'small properties of big systems'. Indeed, we can see complete formal verification as one end of a continuum with traditional forms of static checking (type checking etc.) at the other. Thomas Ball and Sriram Rajamani discussed the impressive success of the SLAM static checker, using theorem proving technology to enhance static checking, which apparently identifies a productive point on this continuum.

One key technique for tackling large and complex problems is*abstraction* , and several speakers discussed the use of abstract interpretation in this capacity. Another powerful technique in real-world problem solving is the identification of certain canonical classes of problems into which many others can be mapped (e.g. propositional satisfiability, linear or semidefinite programming). Armin Biere's talk suggested that quantified boolean formulas (QBF) may become such a class in the near future.

Meanwhile, steady progress on more traditional fronts was reported. For example, Harald Rueß discussed the current techniques and progress made for combining decision procedures for quantifier-free theories, and Ken McMillan surveyed his key idea of using interpolants to allow bounded model checking to be used for complete correctness verification, not merely bug-finding.

A full description of the participants and talks may be found at thelist of talks (`/03451/Proceedings/`). Slides for many of the talks can also be found at this address.

Participants

- Arnold, André (Université Bordeaux)
- Arts, Thomas (IT University of Göteborg)
- Ball, Thomas (Microsoft Corp. – Redmond)
- Basin, David (ETH Zürich)
- Biere, Armin (Universität Linz)
- Cousot, Patrick (ENS – Paris)
- Cousot, Radhia (Ecole Polytechnique – Palaiseau)
- Ganzinger, Harald (-1)
- Garavel, Hubert (INRIA Rhône-Alpes)
- Griffault, Alain (Université Bordeaux)
- Harrison, John (Intel – Hillsboro)
- Hermanns, Holger (Universität des Saarlandes)
- Hungar, Hardi (Universität Oldenburg)
- Hunt, Warren A. (University of Texas at Austin)
- Hutter, Dieter (DFKI – Saarbrücken)
- Maier, Patrick (MPI für Informatik – Saarbrücken)
- McMillan, Ken (Cadence Labs – Berkeley)
- Moore, J Strother (University of Texas at Austin)
- Oostdijk, Martijn (Radboud University Nijmegen)
- Paul, Wolfgang J. (Universität des Saarlandes)
- Paulson, Lawrence (University of Cambridge)
- Peled, Doron A. (University of Warwick)
- Pichora, Mark (MPI für Informatik – Saarbrücken)
- Pnueli, Amir (New York University)
- Podelski, Andreas (MPI für Informatik – Saarbrücken)
- Rajamani, Sriram K. (Microsoft Corp. – Redmond)
- Rueß, Harald (SRI – Menlo Park)
- Rybalchenko, Andrei (MPI für Informatik – Saarbrücken)
- Sagiv, Mooly (Tel Aviv University)
- Schmitt, Peter H. (KIT – Karlsruhe Institute of Technology)
- Schumann, Johann M. (NASA / RIACS – Moffett Field)
- Steffen, Bernhard (TU Dortmund)

– Van Hulst, Marten (Philips Research Europe – Eindhoven)
– Waldmann, Uwe (MPI für Informatik – Saarbrücken)
– Wilhelm, Reinhard (Universität des Saarlandes)
– Yorsh, Greta (Tel Aviv University)
– Zuck, Lenore (University of Chicago)