Executive Summary: Dagstuhl Seminar 10161 on Decision Procedures in Soft, Hard and Bio-ware April 19-23rd, 2010

Nikolaj Bjørner (Microsoft Research)
Robert Nieuwenhuis (Tech. Univ. Catalonia, Barcelona)
Helmut Veith (Vienna University of Technology)
Andrei Voronkov (The University of Manchester)

August 19, 2010

Seminar Goal and Structure

The main goal of the seminar Decision Procedures in Soft, Hard and Bio-ware was to bring together renowned as well as young aspiring researchers from two groups. The first group formed by researchers who develop both theory and efficient implementations of decision procedures. The second group comprising of researchers from application areas such as program analysis and testing, crypto-analysis, hardware verification, industrial planning and scheduling, and bio-informatics, who have worked with, and contributed to, high quality decision procedures. The purpose of the seminar was to heighten awareness between tool and theory developers for decision procedures with the array of applications found in software, hardware and biological systems analysis.

The seminar fell in the week of April 19-23, 2010. In spite of the travel disruptions associated with the Icelandic volcano eruption, 27 researchers from 8 countries (Germany, Austria, Italy, France, USA (who were lucky to arrive late), United Kingdom, Switzerland, and India) arrived and discussed their recent work and future trends. The absence of several attendees from North America, Japan, China and even more distant parts of Europe meant that the seminar was unable to cover planned tutorials on Bio-analysis and constraint solving. Instead it focused heavily on decision procedures in the

Dagstuhl Seminar Proceedings 10161
Decision Procedures in Software, Hardware and Bioware
http://drops.dagstuhl.de/opus/volltexte/2010/2736

context of software analysis and to some extent hardware. On the other hand, it allowed for a highly interactive environment and some attendees got a chance to present a talk on more than one topic. The following summary will have difficulties conveying the very nice spirit of the resulting seminar, but will here summarize the main areas covered during the presentations.

Main Areas Covered during the Seminar

Predicate abstraction and interpolants. When performing symbolic model-checking of software systems, a technique known as predicate abstraction has been instrumental in summarizing large programs as finite abstractions. Theorem provers are critical for computing the abstraction mapping by either producing a predicate cover or using interpolants.

This area received very strong attention, perhaps due to a coincidence of the composition of those who where able to attend. There were five presentations related to interploation:

- Instantiation-Based Interpolation for Quantified Formulae, Jürgen Christ
- Symbol Elimination and Interpolation in Vampire, Krystof Hoder
- Interpolation for Uninterpreted Functions and Linear Arithmetic, Jochen Hoenicke
- Interpolation and Symbol Elimination, Laura Kovacs
- Craig Interpolation for Quantifier-Free Presburger Arithmetic, Philipp Rümmer

Additional abstraction techniques and decision procedures for software analysis were covered as well:

- Computing Abstractions with SMT solvers, Alessandro Cimatti
- The Synergy of Precise and Fast Abstractions for Program Verification, Natasha Sharygina
- Forward Analysis of Depth-Bounded Processes, Thomas Wies
- Software Model Checking via Large-Block Encoding, Alberto Griggio

Hardware verification. Hardware verification has for quite some time now been using propositional logic (SAT) solvers. Even the modern hardware

description languages and methods of their use are, to a large extent oriented toward being verifiable by SAT solvers. However, it seems that SAT-based technology will reach its limits in a few years, so there is an extensive search of higher-level languages and approaches shifting verification from bit-level to word-level and higher. The use of SMT-based decision procedures is emerging in this area.

We asked Professor Armin Biere to prepare a one hour tutorial on the subject of decision procedures in hardware. The result was an enlightening tutorial that covered main trends and challenges in hardware verification. Among the covered areas were word-level decision procedures and symbolic simulation techniques. Both are receiving particular heightened recent attention.

- Decision Procedures in Hardware Design, Armin Biere

Verifying compilers and Synthesis. A verifying compiler uses automated reasoning to check correctness assertions of the program that it compiles. Of significant importance are scaling proofs for verification conditions containing thousands of assumptions, and integrating solvers for several domains.

Of recent interest is also using decision procedures for synthesis. Thanks to a contribution of Ruzica Piskac, the seminar touched briefly on this exciting topic of renewed attention.

- Decision Procedures for Security-by-Contract on Mobile devices, Fabio Massacci
- Verifying Functional Properties with Quantified SMT, Michal Moskal
- Complete Functional Synthesis, Ruzica Piskac

Parametric Systems. Within the context of system verification, an important area of parametric system was discussed in:

- The Model Checker MCMT for Array Based Systems, Silvio Ghilardi
- Hierarchical reasoning for the verification of parametric systems, Viorica Sofronie-Stokkermans

Test-case generation. A technique of recent interest in test-case generation combines runtime analysis with static analysis. It is based on converting

a sequence of instructions, collected at runtime, into a formula, and using a theorem prover for generating inputs that can be used for exercising new execution paths. Theorem provers must be able to handle very large conjunctions of constraints and produce models, for generating new test inputs; in the case the constraints are satisfiable. Besides the challenge of handling very large sets of conjunctions, these tools commonly require the theorem provers to handle bit-precise reasoning, local or global optimization, heap abstractions, and incrementality.

- HAMPI: A Solver for String Constraints, Vijay Ganesh

Decision Procedure Foundations. The many application areas were complemented by in-depth discussions on tools and foundations of decision procedures. Among the foundational topics, the seminar participants contributed with subjects ranging from Quantified Boolean Formulas, the Bernays Shönfinkel class, Linear Rational Programming, Presburger Arithmetic, (hierarchical) local theory reasoning and combinations of Boolean Algebras with Presburger Arithmetic, C_2 and WS1S.

- Decidable fragments of first-order logic, and combinations, Pascal Fontaine
- Hierarchical Reasoning: Improving Efficiency and Ensuring Locality, Swen Jacob
- Quantifier elimination by lazy model enumeration, David Monniaux
- Variable Dependencies of Quantified CSPs, Marko Samer
- Conflict Resolution, Nestan Tsiskaridze
- Decision Procedures for Data Structures, Thomas Wies

Decision Procedure Implementations The foundational material was to some extent complemented with a few implementation oriented contributions:

- The OpenSMT Solver, Roberto Bruttomesso
- Solvers for String Theories, Vijay Ganesh
- Abstract Groebner Bases and Some Applications in Z3 and RAHD, Grant Olney Passmore

Unfortunately, as the Icelandic volcano eruption prevented several participants from overseas, and even more distant parts of Europe, we were unable to cover some of additional relevant and timely topics that were planned. These were noteworthy:

Bio-informatics. Covering new applications for decision procedures in Biology and Medicine.

We had asked Bud Mishra to anchor a section on Bio-informatics. Unfortunately, all flights from North America were canceled at the time of the seminar and he was unable to attend. We are hopeful that he and several other colleagues in the bio-informatics field will be able to participate and contribute in a future seminar.

Scheduling and Planning. Covering advances in SMT procedures that have enabled combining specialized solvers for difference and octagon constraints with efficient combinatorial search taking advantage of search techniques, such as lemma learning and non-chronological back-jumping.

We had asked Robert Nieuwenhuis (a co-organizer) to anchor a tutorial on scheduling and planning applications. This is particularly relevant to the work undertaken in the context of his research group and it is an important vibrant field where recent advances in decision procedures is influencing constraint solvers. Unfortunately, Robert Nieuwenhuis' flight was canceled as well, and he and his group were unable to arrange transportation to the seminar.

Discussion Session

We arranged a discussion session around the topic of software IP and software licensing. This is increasingly relevant as decision procedure implementations, even as they originate in academia, are finding industrial customers. A number of topics were discussed. We just mention two topics touched in the discussion. Armin Biere explained his licensing model for PicoSat and related tools. The tools are released freely under GPL (Gnu Public License), which is condusive for academic research use, but is an impediment for industrial users (from the Hardware sector). He then sells a separate license for industrial use. Nikolaj Bjørner explained how the Micrsoft Research licensing model promotes academic research use of research prototypes, but that different licensing models will be needed for commercial uses. A related issue is the vastly different support models that research prototypes enjoy relative to products that are sustained for several years.

Hike

Wednesday afternoon was spent on a hike around the local lake. While the two participating organizers Helmut Veith and Nikolaj Bjørner were highly enthusiastic of the walk and time near the lake, it was clear from the feedback that other participants were less in favor of a hike. Nevertheless, the organizers found that the hike allowed for informal but very useful technical discussions.

List of participants

Armin Biere, University of Linz; *Nikolaj Bjørner*, Microsoft Research; *Roberto Bruttomesso*, Trento; *Juergen Christ*, Universitæt Freiburg; *Alessandro Cimatti*, Fondazione Bruno Kessler - Trento; *Scott Cotton*, VERIMAG - Gières; *Pascal Fontaine*, INRIA - Nancy; *Vijay Ganesh*, MIT - Cambridge; *Silvio Ghilardi*, Universit di Milano; *Alberto Griggio*, Fondazione Bruno Kessler - Trento; *Krystof Hoder*, University of Manchester; *Jochen Hoenicke*, Universitt Freiburg; *Swen Jacobs*, EPFL - Lausanne; *Laura Kovacs* , TU Wien; *Fabio Massacci*, University of Trento - Povo; *David Monniaux*, VERIMAG - Gières; *Michal Moskal* , Microsoft Research - Redmond; *Grant Olney Passmore*, University of Edinburgh; *Ruzica Piskac*, EPFL - Lausanne; *Philipp Rümmer*, University of Oxford; *Marko Samer*, TU Wien; *Helmut Seidl*, TU München; *Natasha Sharygina*, Universitt Lugano; *Viorica Sofronie-Stokkermans*, MPI fr Informatik - Saarbrücken; *Nestan Tsiskaridze*, University of Manchester; *Thomas Wies*, IST Austria - Klosterneuburg; *Helmut Veith*, TU Vienna;

Links

Dagstuhl main site: `http://www.dagstuhl.de/`
Seminar web site: `http://www.dagstuhl.de/Materials/index.en.phtml?10161`