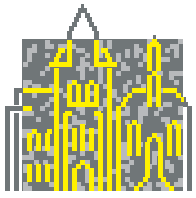
M. Müller-Olm (Univ. Trier, D), H. Riis Nielson (DTU Lyngby, DK),
D. Schmidt (Kansas St. Univ., USA)
(Editors)

Reasoning about Shape

Dagstuhl Seminar 03101 – March 02 to March 07, 2003
Dagstuhl-Seminar-Report No. 369



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

The recent theory and practice of computation has been strongly influenced by aspects of the**shape**(topology) of control, data, and communication structures. Instances of this phenomenon are

- the topology of objects in heap storage;
- the topology of secure networks;
- the topology of communication behavior.

The shape of the resulting topologies can affect and even determine program correctness, reliability, and performance. Different approaches have been developed to reason about such shapes. These approaches have similar aims, face similar technical difficulties, and have achieved similar basic successes, but the connections between the approaches are tenuous and vague.

To address this shortcoming, a Dagstuhl seminar on "Reasoning About Shape" was held on 2-7 March, 2003 that focussed on the topic of reasoning on heap-storage shape as those generated by functional, imperative, and object-oriented programming languages. The seminar was attended by 34 researchers from 8 countries. It brought together three distinct groups of people who use different techniques to study the topic:

- those who use static analysis;
- those who use logics;
- those who use model checking and theorem proving.

In order to facilitate communication between the three communities, four one-hour introductory tutorials were presented on the approaches:

1. **"An Introduction to Shape Analysis"**
   (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.RepsThomas.2.Abstract.txt`)
   by Thomas Reps, University of Wisconsin[Slides]
   (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.RepsThomas.2.Slides.pdf`)
2. **"An Introduction to Separation Logic"**
   by Josh Berdine, Queen Mary University, London
3. **"An Introduction to Model Checking and Flow Analysis"**
   (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.Mueller-OlmMarkus.Abstract.txt`)
   by Markus Müller-Olm, Universität Dortmund[Slides]
   (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.Mueller-OlmMarkus.Slides.pdf`)

4. **"An Introduction to Heap-abstraction Methods"** (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.SchmidtDavid.Abstract.txt`)
   by David Schmidt, Kansas State University[Slides]
   (`http://www.dagstuhl.de/files/Proceedings/03/03101/03101.SchmidtDavid.Slides.pdf`)

The topics in the tutorials were developed by 24 technical presentations by the seminar participants. The seminar format provided ample time for discussion and development: each one-hour tutorial was followed by 20 minutes of discussion, and each 30-minute technical presentation was followed by 15 minutes of discussion. (Often, the discussion was intermixed with the presentation.)

All talks will appear in the Online Proceedings (`http://www.dagstuhl.de/files/Proceedings/03/03101/`).

Scientific Highlights

Several significant areas of study were developed by the technical speakers. Noteworthy (but not exhaustive) examples were

- improvement of static heap analysis, as presented by Greta Yorsh, Tel Aviv University ("Symbolic characterization of heap abstractions"), Eran Yahav, Tel Aviv University ("Use of evolution logic for verifying temporal properties of concurrent software"), and Thomas Reps, University of Wisconsin ("Symbolic implementation of the 'Best' transform")

- development of logic-based approaches to reasoning about heap storage, for example, Hongseok Yang, KAIST University, Korea ("Verification of the Schorr-Waite graph marking algorithm by refinement"), Peter O'Hearn, Queen Mary College, London ("Local reasoning and the frame rule"), and Cristiano Calcagno, Imperial College London ("Automatic reasoning of programs in spatial logic")

- application of model-checking and theorem-proving techniques, presented by Helmut Seidl, Trier Universität ("Linear algebra for program analysis," Anders Møller, Aarhus Universitet ("Program verification with monadic second-order logic"), Patrick Maier, Max-Planck-Institut für Informatik, Saarbrücken ("Bounded model checking of pointer programs"), and Andreas Podelski, Max-Planck-Institut für Informatik, Saarbrücken ("Software model checking for safety and liveness")

Two other significant contributions must be mentioned: Martin Rinard, Massachusetts Institute of Technology, presented a talk on "Data structure consistency checking and repair," and Viktor Kuncak, also of MIT, spoke about "The undecidability of graph matching in monadic second-order logic." The latter talk demonstrated a negative result that impacts one direction of work followed by the static-analysis shape community and was a significant contribution made available by the Dagstuhl seminar.

Perspectives

In addition to the significant scientific contributions presented at the meeting, the seminar provided an important opportunity for the members of the three approaches to be exposed to the work of the other groups and discuss similarities, differences and potential for collaboration. After five days of presentations, discussions, and debates, two meetings were held to summarize the results of the seminar. Briefly stated, the conclusions are the following.

- Shape analysis is a viable research field with substantial intellectual content and significant applications and problems waiting to be solved. There are promising solutions and a community is building around the topic. The Dagstuhl seminar was a significant contribution to the development of that community.
- The field of shape analysis is not mature. As demonstrated at the seminar, there are many approaches, and it is unclear how to evaluate and compare the approaches. Nonetheless, it is important to proceed, because the topic is one of the last important semantical problem in the core imperative programming field.
- Future concerns must include applying existing approaches to larger problems, especially by exploiting abstraction and modularity principles. There is an uncertainty as to the degree of manual annotation versus automated inference that can be applied to solving the problem. Finally, more time must be spent on deciding upon those crucial shape properties that must be solved and developing the technology to deduce the crucial properties. The interactions between the three communities at the workshop were an impressive start, but more collaboration will be required.

Program Organizers

Markus Müller-Olm (`http://ls5-www.cs.uni-dortmund.de/~mmo/`)(Universität Dortmund, Germany)
Hanne Riis Nielson (`http://www.daimi.aau.dk/~hrn/`)(DTU Lyngby, Denmark)
David A. Schmidt (`http://www.cis.ksu.edu/~schmidt/`)(Kansas State University, USA)

Participants

- Banerjee, Anindya (Kansas State University)
- Berdine, Joshua (Queen Mary University of London)
- Blanchet, Bruno (ENS – Paris)
- Bornat, Richard (Middlesex University)
- Calcagno, Cristiano (Imperial College London)
- Cousot, Radhia (Ecole Polytechnique – Palaiseau)
- Hähnle, Reiner (Chalmers UT – Göteborg)
- Huth, Michael (Imperial College London)
- Kreiker, Jörg (Universität des Saarlandes)
- Kuncak, Viktor (MIT – Cambridge)
- Lee, Oukseh (KAIST – Daejeon)
- Loginov, Alexey (University of Wisconsin – Madison)
- Maier, Patrick (MPI für Informatik – Saarbrücken)
- Manevich, Roman (Tel Aviv University)
- Müller-Olm, Markus (Universität Münster)
- Møller, Anders (Aarhus University)
- Naumann, David A. (Stevens Institute of Technology)
- O'Hearn, Peter (Queen Mary University of London)
- Podelski, Andreas (MPI für Informatik – Saarbrücken)
- Reddy, Uday (University of Birmingham)
- Rehof, Jakob (Microsoft Corp. – Redmond)
- Reps, Thomas W. (University of Wisconsin – Madison)
- Rinard, Martin C. (MIT – Cambridge)
- Rüthing, Oliver (TU Dortmund)
- Sagiv, Mooly (Tel Aviv University)
- Schmidt, David (Kansas State University)
- Seidl, Helmut (TU München)
- Sims, Elodie-Jane (Ecole Polytechnique – Palaiseau)
- Thielecke, Hayo (University of Birmingham)
- Vogel, Nelson (University of Sao Paulo)
- Wilhelm, Reinhard (Universität des Saarlandes)
- Yahav, Eran (Tel Aviv University)

– Yang, Hongseok (Seoul National University)
– Yi, Kwangkeun (Seoul National University)
– Yorsh, Greta (Tel Aviv University)