08061 Executive Summary
Types, Logics and Semantics for State
— Dagstuhl Seminar —

Amal Ahmed[1], Nick Benton[2], Martin Hofmann[3] and Greg Morrisett[4]

[1] Toyota Technological Inst. - Chicago, USA
amal@tti-c.org
[2] Microsoft Research, GB
nick@microsoft.com
[3] Universität München, D
mhofmann@informatik.uni-muenchen.de
[4] Harvard University, USA
greg@eecs.harvard.edu

Abstract. From 3 February to 8 February 2008, the Dagstuhl Seminar 08061 State" Conference and Research Center (IBFI), Schloss Dagstuhl. 45 researchers, with interests and expertise in many different aspects of modelling and reasoning about mutable state, met to present their current work and discuss ongoing projects and open problems.

Keywords. Mutable State, Program Logics, Semantics, Type Systems, Program Analysis

1 Introduction

The combination of dynamically allocated, mutable data structures and higher-order features is present in almost all programming languages, from C to ML, Java and C♯. The search for good models and reasoning principles for, and language features that tame the complexity of, this combination goes back many decades. Recent years have seen a number of significant advances in our semantic understanding of state and encapsulation, including the development of separation logic, substructural type systems, models using parametric logical relations, and new bisimulation-based reasoning methods.

At the same time, concern about reliability, correctness and security of software has led to increased interest in tool and language support for specification and verification of realistic languages (for example JML and Spec♯), certified and certifying compilation, proof-carrying code, safe systems programming languages (such as Cyclone and CCured), and practical type systems capturing and controlling subtle aspects of state, such as ownership, effects, information flow and protocol conformance.

The seminar brought together researchers working on all aspects of state in programming languages, with the aim of developing closer links between the

Dagstuhl Seminar Proceedings 08061
Types, Logics and Semantics for State
http://drops.dagstuhl.de/opus/volltexte/2008/1426

theoretical and applied lines of work, and laying groundwork for advances in the state of the art in both.

This is an exciting and important research area. Mathematically sound reasoning principles for state, combined with recent advances in program analysis and machine-assisted proof, have the potential to lead to improved programming languages, compilers, verification technology and even to new approaches to software deployment and operating system design. Using flexible, certified language-based approaches to encapsulation and security in place of hardware protection is a promising idea; systems such as Singularity and House (and, indeed, the JVM and CLR) have already taken steps in this direction.

Among the research challenges addressed at the seminar were:

- How do we integrate state and effects into dependently typed languages and how that might inform the design of tools and specification languages such as JML?
- What are the semantic foundations of existing logics and type systems for ownership, confinement, effects and permissions, and how may such foundations be used not only to understand and improve these systems, but also to relate them formally to one another?
- How should we model and reason soundly about concurrency, locks and transactions?
- How can we reason about controlled use of state at multiple levels of abstraction, for example in relating high-level, language-enforced restrictions to low-level guarantees on the behaviour of compiled code?
- What is the right mix of approaches to the control of state and other effects? How do we balance language design and type systems, automated verification tools and machine assisted proof?

2 Participation and Programme

The seminar brought together 45 researchers from Europe, the United States and Israel with interests and expertise in many different aspects of modelling and reasoning about mutable state. There were about 40 talks over the course of the week (see the associated abstracts collection), comprising invited overview talks on particular topics, ordinary contributed talks (mostly on recent, completed work) and shorter, more informal talks on open problems and issues that arose during the week.

A major goal of the seminar was to forge links between researchers working on related problems from different perspectives. This was certainly achieved, with talks covering almost all combinations of semantic models, program logics, reasoning principles, program analyses and rich type systems for state in high-level and low-level, functional, imperative and object-oriented, sequential and concurrent, programming languages.

There was a clear sense of significant recent progress being made, on both the theoretical and applied aspects of reasoning about state. Separation logic, step-indexing and FM-domains are all recent developments with the first, in

particular, having had a significant impact on much of the research discussed at the seminar. Fully automatic program analyses (such as pointer analyses) and machine-assisted proof have both advanced tremendously this century, to the extent that a number of projects are working on formal verifications of systems code that would have been considered impractical just a decade ago.

At the same time, some very interesting and useful technical interactions at the seminar concerned more elementary methodological questions. The definitions of, distinctions between and necessity of ghost variables, auxiliary variables, model variables and logic variables generated much discussion, as did the question of prescriptive versus descriptive readings of preconditions in triples and intensional versus extensional program properties.

This was an intense and productive week. With a relatively large number of particpants, most of whom wanted to speak, scheduled talks took up most of the days, including part of the traditional 'afternoon off' on Wednesday. Informal discussions continued into the night throughout the week.

The organizers and participants thank the staff and management of Schloss Dagstuhl for their assistance and support in the arrangement of a very successful meeting.