7th Wessex Theory Seminar

The seventh meeting of the Wessex Theory Seminar took place on Wednesday 14th April 2010, at the University of Bath, starting with lunch from 12.15pm.

Programme

12.15 - 1.15 Lunch (Claverton Rooms)

1.15 - 2.15 Paul Levy: Nondeterminism, fixpoints and bisimulation

2.15 - 3.00 Yoshiki Kinoshita: Hoare in Agda

3.00 - 3.30 Break

3.30 - 4.15 Guy McCusker: Modelling local variables: possible worlds and object spaces

4.15 - 5.00 Temesghen Kahsai: Property preserving development and testing for Csp-Casl

5.00 - 5.30 Makoto Takeyama: Assurance Cases in Agda

Abstracts

Paul Levy

Nondeterminism, fixpoints and bisimulation

Denotational semantics of nondeterminism is an old subject, but many fundamental problems remain, such as modelling bisimulation and fairness. This talk is a survey of the state of the art in these problems.

On the one hand, we see counterexamples that pinpoint the difficulties. On the other, I will indicate some lines of investigation that appear promising, using recent technology such as game semantics and operational reasoning methods.

Yoshiki Kinoshita

Hoare in Agda

I will talk about our shallow embedding of Hoare Logic in
Agda, which may also be regarded as soundness proof of Hoare Logic
written in Agda. This is joint work with Makoto Takeyama.

Guy McCusker

Modelling local variables: possible worlds and object spaces

Local variables in imperative languages have been given denotational
semantics in at least two fundamentally different ways. One is by use
of functor categories, focusing on the idea of possible worlds.
The other might be termed event-based, exemplified by Reddy's
object spaces and models based on game semantics. O'Hearn and Reddy
have related the two approaches by giving functor category models
whose worlds are object spaces, then showing that their model is fully
abstract for Idealised Algol programs up to order two. But the
category of object spaces is not small, and so their functor category
is unlikely to be locally small. That means they cannot use the body
of results flowing from local smallness, such as cartesian closedness
of the functor category and its implications for their model. In this
talk we show how to refine their model by proving that the finite objects form a
small dense subcategory of a simplified object-spaces model, making
the induced functor category locally small, at the expense of being forced
to work in a Cpo-enriched setting.

Temesghen Kahsai

Property preserving development and testing for Csp-Casl

In this talk I will illustrate some development notions for the
specification language Csp-Casl. The latter is a specification language
that allows to specify data and processes in an integrated way.
These development notions are capable of capturing informal vertical

and horizontal software developments which we typically find in industrial applications (e.g. electronic payment system).
On the other hand, such development notions allow us to verify some interesting properties, e.g., deadlock or livelock freedom.

I will also present a theory for the evaluation of test cases with respect to Csp-Casl specifications. With this approach, it is possible to develop test cases for even the most abstract and basic specifications, and to reuse them later on in more refined systems.

The presented theoretical results have been applied to the electronic payment system EP2. Here, we have modeled the system in Csp-Casl, verified properties using tool support and finally tested the system in an hardware-in-the-loop testing framework.

Makoto Takeyama

Assurance Cases in Agda

Assurance Cases are a key concept in communicating assurance of computer systems' dependability among the stakeholders. They make explicit arguments for claims on systems properties with supporting evidences. They are large and complex documents that are hard to construct and evaluate. We aim to introduce automation by formalising cases as proofs in Agda. The adequacy of formalization process itself becomes a problem for each case. We discuss writing styles for cases in Agda that enables detailed review of the formalization by assessors.

Attendance

From AIST (Japan):

- Yoshiki Kinoshita
- Makoto Takeyama

From Birmingham:

- Paul Levy

From Bath:

- Ana C. Calderon
- Martin Churchill
- Jim Laird
- Guy McCusker
- John Power

From Swansea:

- Phillip James
- Temesghen Kahsai
- Fredrik Nordvall Forsberg
- Liam Oreilly

From Oxford:

- Nikos Tzevelekos

From Southampton:

- Ross Horne
- Gabrielle Anderson
- Toby Wilkinson