2nd Wessex Theory Seminar

The second meeting of the Wessex Theory Seminar was held on Wednesday 17 September 2008, hosted by the University of Bath. Lectures were held in Room 6E 2.2 of the University of Bath's Claverton (Bath) campus.

Lunch and coffee were provided.

Talks were expected to last 35-40 minutes, giving time for questions and change-over. The schedule for the day was as follows, with abstracts below:

Programme

11:00 Coffee

11:15 Peter Mosses: Implicit Propagation in SOS

12:00 Lunch

1:30 Keishi Okamoto: Formalization of System LSI Specification and Automatic Generation of Verification Items
2:15 Arnold Beckmann: On the Complexity of Parity Games

3:00 Coffee

3:30 Shunsuke Yatabe: A new project on formalizing specifications
4:15 Anton Setzer: Proofs by Guarded Recursion

5:00 Close

Attendance

From AIST (Japan):

Keishi Okamoto
Shunsuke Yatabe

From Bath:

Ana C. M. Abbud
Paola Bruscoli
Martin Churchill
James Davenport
Jim Laird
Guy McCusker
John Power

From Oxford:

Chris Broadbent

From Southampton:

Ross Horne

From Swansea:

Arnold Beckmann
Jin Cao
Karim Kanso
Oliver Kullmann
Ebrahim Larijani
Peter Mosses
Mark New
Monika Seisenberger
Anton Setzer

Abstracts

Arnold Beckmann (joint work with Faron Moller): On the complexity of parity games (BM08)

> *Abstract: Parity games underlie the model checking problem for the modal ¿-calculus, the complexity of which remains unresolved after more than two decades of intensive research. The community is split into those who believe this problem - which is known to be both in NP and coNP - has a polynomial-time solution (without the assumption that P=NP) and those who believe that it does not. (A third, pessimistic, faction believes that the answer to this question will remain unknown in their lifetime.)*
>
> *In this paper we explore the possibility of employing Bounded Arithmetic to resolve*

> *this question, motivated by the fact that problems which are both NP and coNP, and where the equivalence between their NP and coNP description can be formulated and proved within a certain fragment of Bounded Arithmetic, necessarily admit a polynomial-time solution. While the problem remains unresolved by this paper, we do proposed another approach, and at the very least provide a modest refinement to the complexity of parity games (and in turn the ¿-calculus model checking problem): that they lie in the class of Polynomial Local Search problems. This result is based on a new proof of memoryless determinacy which can be formalised in Bounded Arithmetic.*
>
> *The approach we propose may offer a route to a polynomial-time solution. Alternatively, there may be scope in devising a reduction between the problem and some other problem which is hard with respect to PLS, thus making the discovery of a polynomial-time solution unlikely according to current wisdom.*

Peter Mosses (joint work with Mark New): Implicit Propagation in SOS (MN08)

> *Abstract: In contrast to a transition system specification in process algebra, a structural operational semantics (SOS) of a programming language usually involves auxiliary entities: stores, environments, etc. When specifying SOS rules, particular auxiliary entities often need to be propagated unchanged between premises and conclusions. The standard technique is to make such propagation explicit, using variables. However, referring to all entities that need to be propagated unchanged in each rule can be tedious, and it hinders direct reuse of rules in different language descriptions.*
>
> *We propose a new interpretation of SOS rules, such that each auxiliary entity is implicitly propagated in all rules in which it is not mentioned. The main benefits include significant notational simplification of SOS rules and much-improved reusability. This new interpretation of SOS rules is based on the same foundations as Modular SOS, but avoids the notational overhead of grouping auxiliary entities together in labels.*
>
> *After motivating and explaining implicit propagation, we consider the foundations of SOS and Modular SOS specifications, and define the meaning of SOS specifications with implicit propagation by translating them to Modular SOS. We then show how implicit propagation can simplify various rules found in the SOS literature.*

Keishi Okamoto: Formalization of System LSI Specification and Automatic Generation of Verification Items

> *Abstract:The design process of a system LSI traditionally starts with an informal specification in a combination of a natural language and some pseudo programming language such as a pseudo C. This informal specification is used to generate items for verification of lower-level detailed designs. Engineers generating those verification items often face the problems of informality. Ambiguities, implicit assumptions, inconsistencies, etc. in the specification lead to wrong verification items or critical omission. Informality means that the generation is basically a manual process prone to simple errors. Besides those reliability issues, the cost of manual generation is a big issue in the productivity of design processes.*
>
> *We aim at automatic generation of verification items from specifications. The target specification for this study is that of a system LSI under development at Renesas Technology Corp.*

Anton Setzer: Proofs by Guarded Recursion

> *Abstract: Martin-Löf type theory (MLTT) is based on the dependent function type and (inductively defined) algebraic types. In order to model concepts like interaction or object-orientation in MLTT in a direct way, it is useful to add (coinductively defined) weakly final coalgebras to MLTT.*
> *We introduce formation, introduction, elimination, and equality rules for weakly final coalgebras in MLTT. We will show that guarded induction is nothing but an informal description of the introduction rules for weakly final coalgebras.*
> *We investigate the duality between algebraic and coalgebraic types in those rules: For algebraic types the introduction rules are simple and predicative, the elimination rules involve some degree of impredicativity.*
> *There is a large variety of possible elimination rules, all of which are derived from the principle of having a least set closed under the introduction rules.*
> *For coalgebraic types, the elimination rules are simple and predicative, whereas the introduction rules involve some degree of impredicativity. There is a large variety of possible introduction rules, all of which are derived from the principle of having the largest set allowing the elimination principle.*
>
> *We introduce a model of the extension of MLTT by weakly final coalgebras, and investigate the implications for meaning explanations, namely the need for types, the meaning of which is given by an elimination principle.*
>
> *We will then show that bisimulation is an example of a dependent weakly final coalgebra. We demonstrate that proofs by guarded induction of bisimulation form a much more intuitive way of proving bisimulation properties than the usual proofs based on the introduction of a bisimulation relation.*

Shunsuke Yatabe: A new project on formalizing specifications

> *Abstract: In this talk we introduce a new on-going research project (jointly with several companies) for developing a methodology and software tools that can improve the upper development scene of software product.*
> *This aims to formalize a unified form of specifications of Embedded Software in a proof assistant system Agda, and develop tools which assist in writing such formalized specifications.*