MPhil in Advanced Computer Science
Interactive Formal Verification

Leader:	Lawrence Paulson (course lecturer)
Timing:	Lent
Prerequisites:	familiarity with basic logic and operational semantics
Structure:	12 Lectures and 4 Practical Classes

AIMS

This module introduces students to interactive theorem proving using Isabelle. It includes techniques for specifying formal models of software and hardware systems and for deriving properties of these models.

SYLLABUS

1. Introduction to higher-order logic. Verifying simple functional programs. (1 Lecture)
2. Recursive datatypes and functions: modelling them in logic, reasoning about them. (1L)
3. Simplification heuristics. (1L)
4. Logical reasoning: how to generate proofs that involve quantification, case analysis, etc. (2L)
5. Set-theoretic primitives, notation and reasoning methods. (1L)
6. Introduction to hardware verification: combinational and sequential circuits, registers, etc. (2L)
7. Modelling operational semantics definitions and proving properties. (2L)
8. Structured proofs. (2L)

OBJECTIVES

On completion of this module students should

- possess basic skills in the use of Isabelle
- be able to specify inductive definitions and perform proofs by induction
- be able to verify simple hardware circuits
- be able to express a variety of specifications in higher-order logic

COURSEWORK

Each candidate will undertake a small formalisation, which will serve as the basis for assessment.

PRACTICAL WORK

Four supervised practical sessions will allow students to develop skills.

ASSESSMENT

Each student must undertake a small verification project, delivering a practical write-up accompanied by an Isabelle theory file. It will be started during the practical sessions but will probably be completed on the student's own time. The project will assess the extent to which each candidate has absorbed the syllabus and develop practical skills. The lecturer will set and mark the assessments. The mark will be reported as a percentage.

RECOMMENDED READING

- Tobias Nipkow, L. C. Paulson and Markus Wenzel. Isabelle/HOL: A Proof Assistant for Higher-Order Logic (Springer LNCS 2283, 2002).
- Alexander Krauss, Defining Recursive Functions in Isabelle/HOL
- Tobias Nipkow, A Tutorial Introduction to Structured Isar Proofs

Last updated: January 2009