Distributed Systems Programming F21DS1

Formal Methods for Distributed Systems

Andrew Ireland

School of Mathematical and Computer Sciences
Heriot-Watt University
Edinburgh

Knowledge: Broad & Shallow

- Formal Methods for Distributed Systems:
  - Motivations
  - Applicability
- Formal Verification:
  - The process of formal verification, *i.e.* modelling, specification and analysis.
  - Modelling: functional, relational, abstract machines, automata, object-oriented.
  - Specification: complete and property based.
  - Analysis: equivalence checking, model checking, theorem proving.

Knowledge: Narrow & Deep

- The Promela modelling language.
- SPIN's analysis capabilities:
  - Random & interactive simulation.
  - Assertion verification (local & global).
  - Validation labels (end-states, progress & acceptance).
  - Temporal verification: generic properties, *i.e.* invariance, response and precedence.
  - Fairness issues.
  - An understanding of how SPIN's model checker works, i.e. how system models and LTL properties are represented, and how LTL reasoning is implemented.

Essential Skills

- To be able to understand and develop models of distributed communicating systems in Promela.
- To be able to understand and write specifications for Promela models using SPIN's various reasoning capabilities.
- To be able to predict and interpret the results generated by SPIN's verifier.
- To be able to construct an automata based representation for a very simple Promela model.
- To be able to convert between LTL formulas and Buchi automata.