Incremental Design of Distributed Systems

Michael Butler
University of Southampton, United Kingdom

These lectures will build on those presented by Jean-Raymond Abrial on Methods and Tools for System and Software Construction. In particular the lectures will make use of Event-B for modelling and refinement and make use of the Rodin toolset for Event-B.

It will shown how Event-B can be use to model and reason about distributed systems from a high-level global view down to a detailed distributed architectural view. It will be shown how refinement and decomposition can be used to introduce distribution of state and control and to introduce message passing between components.

Performing refinement in incremental steps means that the abstraction gap between refinement levels is not too great. This means that the proof effort can be factored out into many relatively simple steps. Simple proof steps allow for a high degree of automation in proof.

A key ingredient in performing refinement proofs is the gluing invariant linking states of abstraction levels. A key role of the proof obligations generated by the Rodin tool are to verify the maintainence of gluing invariants. But the tool can also be used to help in the discovery of appropriate gluing invariants.

A link between modelling in Event-B and modelling with process algebra such as CSP will be made. Typically in process algebra the behaviour of a process is defined in terms of the events in which it can engage. A similar view can be taken of Event-B models and has a bearing on the way in which interaction, composition and refinement are treated. The relationship to modelling and proof in Event-B will be outlined.

The exposition will mostly be based around some examples of distributed systems including

- a distributed access control mechanism;
- a replicated database system;
- an electronic funds transfer system.

References

1. Butler, M. and Yadav, D. *An Incremental Development of the Mondex System in Event-B.* Formal Aspects of Computing, 20 (1); pp 61–77; 2008.
`http://eprints.ecs.soton.ac.uk/13346/`
2. Butler, M. J. *Stepwise Refinement of Communicating Systems.* Science of Computer Programming, 27 (2); pp 139–173; 1996.
`http://eprints.ecs.soton.ac.uk/575/`