Executable Formal Models in Rewriting Logic

Carolyn Talcott

SRI International
Menlo Park, California, USA
clt@csl.sri.com

Abstract

Formal executable models provide a means to gain insights into the behavior of complex distributed systems. Ideas can be prototyped and assurance gained by carrying out analyses at different levels of fidelity: searching for desirable or undesirable behaviors, determining effects of perturbing the system, and eventually investing effort to carry out formal proofs of key properties. This modeling approach applies to a wide range of systems, including a variety of protocols and networked cyber-physical systems. It is also emerging as an important tool in understanding many different aspects of biological systems.

Rewriting logic (RWL) is a formalism that is well-suited to developing and working with formal executable models. In RWL term rewriting is used to represent both structure (equational properties and functions) and transformation / behavior. Logics and inference systems can be naturally represented in RWL, as can the structure and behavior of distributed systems both engineered and natural.

Maude is a high performance realization of Rewriting Logic. Maude specifications are naturally executable and the Maude environment provides a variety analysis tools to reason about properties of models. These include reachability analysis, symbolic execution (narrowing), and model-checking. In addition, Maude is reflective. This provides a powerful mechanism for extension.

The talk will present a sampling of executable specifications using Maude and its extensions. The examples will illustrate a range of modeling problems and analysis approaches, including

- Analysis of engineered systems
  - finding problems and fixing the system,
  - optimizing performance.
- Analysis of natural systems
  - finding problems and fixing the model,
  - using the model to predict consequences of perturbations.

To be self-contained, the talk will begin with a little introduction to RWL and Maude.

1998 ACM Subject Classification D.2.4 Formal methods, F.3.1 Specification techniques, mechanical verification

Keywords and phrases Executable model, formal analysis, rewriting logic

Digital Object Identifier 10.4230/LIPIcs.RTA.2015.22

Category Invited Talk

26th International Conference on Rewriting Techniques and Applications (RTA'15).
Editor: Maribel Fernández; pp. 22–22

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany