Abstract

Designing Cyber-Physical Systems is hard. Physical testing can be slow, expensive and dangerous. Furthermore computational components make testing all possible behavior unfeasible. Model-based design mitigates these issues by making it possible to iterate over a design much faster. Traditional simulation tools can produce useful results, but their results are traditionally approximations that make it impossible to distinguish a useful simulation from one dominated by numerical error. Verification tools require skills in formal specification and a priori understanding of the particular dynamical system being studied.

This thesis presents rigorous simulation, an approach to simulation that uses validated numerics to produce results that quantify and bound all approximation errors accumulated during simulation. This makes it possible for the user to objectively and reliably distinguish accurate simulations from ones that do not provide enough information to be useful. Explicitly quantifying the error in the output has the side-effect of leading to a tool for dealing with inputs that come with quantified uncertainty.

We formalize the approach as an operational semantics for a core subset of the domain-specific language Acumen. The operational semantics is extended to a larger subset through a translation. Preliminary results toward proving the soundness of the operational semantics with respect to a denotational semantics are presented. A modeling environment with a rigorous simulator based on the operational semantics is described. The implementation is portable, and its source code is freely available. The accuracy of the simulator on different kinds of systems is explored through a set of benchmark models that exercise different aspects of a rigorous simulator. A case study from the automotive domain is used to evaluate the applicability of the simulator and its modeling language. In the case study, the simulator is used to compute rigorous bounds on the output of a model.