MURI Research Report 2010-2011

B. Krogh

Architectural Modeling

We developed an extension of existing software architecture tools to model physical systems, their interconnections, and the interactions between physical and cyber components. To support the principled design and evaluation of alternative architectures for cyber-physical systems (CPSs), a new CPS architectural style has been developed. The implementation in AcmeStudio includes behavioral annotations on components and connectors using either finite state processes (FSP) or linear hybrid automata (LHA) with plug-ins to perform behavior analysis using the Labeled Transition System Analyzer (LTSA) or Polyhedral Hybrid Automata Verifier (PHAVer), respectively.

in year 5 we continued the development of an architectural approach to multi-modeling for the development of complex embedded control systems. Models in heterogeneous formalisms are related by associating each model with an architectural view of a base architecture. Structural consistency is evaluated through the analysis of graph morphisms, with algorithmic methods for identifying inconsistencies in connectivity and encapsulations. These methods have been applied to the analysis of multiple heterogeneous models of the STARMAC quadrotor system. We have also performed an architectural analysis and restructuring of the lower-level control system for the quadrotor in our laboratory. We also developed a new approach to specifying and analyzing semantic consistency between models through the evaluation of logical conditions on the constraints on model parameters. Plug-ins for both structural and semantic consistency are being developed during the last months of the project.

Advances in Verification and Reachability Analysis

Reachability computations are foundational to the verification of continuous and hybrid dynamic systems. In this MURI we made several advances in the development of reachability analysis techniques for continuous and hybrid dynamic systems. We extended the concept of counterexample guided abstraction refinement (CEGAR) techniques in the verification of discrete systems to hybrid systems. In a new method called iterative relaxation analysis, multiple abstractions are constructed such that the composition of the results for the collection of abstractions leads to a successful verification of the overall system. This approach out-performs state-of-the-art reachability engines by a factor of 1000 on some examples.

We also developed reachability-based methods for verifying properties of numerical software, taking into account floating point errors. The technique uses a new widening operator, similar to the types of operators used to guarantee convergence to a fixed point in abstract interpretation. We developed a new bounded-time verification technique that combines software model checking and simulation. The technique directly analyzes controller code and reachable set estimation via bisimulation functions is used to conservatively capture the behaviors of a plant with continuous dynamics. We have also developed a new method for finding counterexamples that uses a software model checker to perform a systematic simulation of the software implementation of a controller coupled with a continuous plant.

In year 5 developed new methods for computing tight overapproximations of reachable sets for linear dynamic systems with uncertain, time-varying parameters and bounded input signals. This makes it possible to compute much tighter approximations to reachable sets for nonlinear systems using on-the-fly local linearizations. Using zonotopes as the fundamental representation of sets, reachable sets can be computed for systems with dozens of continuous state variables. Improvements of two to three orders of magnitudes in computation times have been achieved.

Publications since the last report

A. Bhave, B. H. Krogh, D. Garlan, B. Schmerl, Multi-domain modeling of cyber-physical systems using architectural views, Analytic Virtual Integration of Cyber-Physical Systems Workshop, San Diego, CA, Nov 2010.

J. Kapinski, B. H. Krogh, On incrementally bounded systems, American Control Conference (ACC), Baltimore, MD, July 2010, pp. 6348 - 6350.

M. Althoff, C. Le Guernic, B. H. Krogh, Reachable set computation for uncertain time-varying linear systems, Conference on Hybrid Systems: Computation and Control (HSCC), Chicago, IL, Apr 2011.

A. Bhave, B. H. Krogh, D. Garlan, B. Schmerl, View consistency in architectures for

cyber-physical systems, International Conf. on Cyber-Physical Systems (ICCPS), Chicago, IL, Apr 2011.