Editorial: Special Section VCPSS'09

This special section on Numerical Verification of Cyber-Physical Software Systems comes as a follow-up to a successful series of workshops and special issues on Numerical Software Verification. At the time this editorial was written, the International Workshop on Numerical Software Verification (NSV) had already reached its third successful instantiation. In detail, NSV-I was held in July 2008 along with the Computer-Aided Verification (CAV) conference at Princeton, NJ. NSV-II was held in April 2009 as part of the CPSWeek in San Francisco, CA, and it was affiliated with the International Conference on Hybrid Systems: Computation and Control. The latest in the series, NSV-III was held in July 2010 in Edinburgh, Scotland, and it was part of the Federated Logic Conference (FLoC 2010) and affiliated with CAV 2010 and the Symposium on Logic in Computer Science (LICS) 2010. Finally, NSV-I spurred a special issue on Formal Methods in System Design.

The goal of the NSV series of workshops and special issues is to spark interest in and focus attention on research problems that relate to numerical issues of general purpose software. Even though numerical issues relating to computation have been extensively studied within the scientific computing community, the proof of correctness of general or specific purpose software under such issues is still in its infancy. The special section at hand focuses even further on issues relating to software for Cyber-Physical Systems (CPS). The issue contains 6 articles that cover a wide range of applications within the verification of software and models of CPS.

The article by Tichakorn Wongpiromsarn, Sayan Mitra, Andrew Lamperski and Richard Murray studies the problem of verifying embedded control software for autonomous ground vehicles. In this work, the authors introduce a new modeling formalism for hybrid systems that particularly targets periodically controlled embedded systems. Empirically, most real-life implementations of hybrid systems could be described using that modeling formalism. Then, the authors derive sufficient conditions for proving safety properties of hybrid systems that fall within the class of Periodically Controlled Hybrid Automata (PCHA). For certain classes of PCHA such invariance verification can be performed automatically. One of the highlights of the article is the application of the proposed method to the manual verification of the controller of Alice, the California Institute of Technology autonomous ground vehicle entry to the 2007 DARPA Urban Challenge. Using their new framework, the authors determined that the failure that Alice exhibited during the Urban Challenge was due to an unfortunate choice of certain system parameters rather than some algorithmic or logic failure in the design.

The article by Antoine Girard and Gang Zheng presents their work on verifying safety and liveness properties of metric transition systems. The basic idea behind their approach consists of using model-checking for infinite state systems wherein a metric bisimulation is used to capture the currently explored behavior by considering "nearby" behaviors that also have the same outcome with respect to the property being verified. Metric bisimulations are natural for cyber-physical systems since they make essential use of the continuity in the state-space of the system to make deductions about system properties. The authors demonstrate the practical aspects of their work on the verification problem of an embedded control system. One of the advantages of the work by Girard and Zheng is that it can be applied to synthesis problems as well.

DOI 10.1145/2331147.2331162 http://doi.acm.org/10.1145/2331147.2331162

The article by Sanjit Seshia and Alexander Rakhlin analyzes quantitative properties of systems using game-theoretic learning. The authors introduce a framework to estimate with high probability a numerical property of a system using measurements from tests. In detail, the system is assumed to be modeled by a weighted directed acyclic graph, whose weights might be altered by the environment, where the numerical quantity depends on the particular path chosen on the graph. The authors take a game-theoretic approach where they try to learn a model of the system by playing a game between the environment, which chooses the disturbances, and the system, which chooses the inputs. The goal of the article is to try to estimate the worst-case and average-case value of the quantity. The relevance of the article to this special section is through the application of the proposed method, namely, the authors demonstrate their approach on the estimation of the Worst-Case Execution Time (WCET) problem for embedded software. WCET estimation is a very important problem for verifying that the software can be scheduled for execution on a platform without missing any deadlines. Toward that goal, the authors have implemented a WCET estimation toolbox called GameTime. Among the benefits of GameTime are its portability and its application to the actual platform rather than a model of the system. The results of the article demonstrate that this is a very promising approach of WCET estimation for soft real-time as well as for hard real-time computing applications.

The article by Lan Wu and Wei Zhang presents one of the first applications of model checking to estimating the WCET of multicore processors. In detail, the authors focus on the WCET problem of independent threads running on multicore processors with a shared L2 instruction cache. They model each concurrent process and their potential interferences in the shared cache within SPIN. Then, they bound the WCET by performing a binary search, and they propose a number of modeling simplifications that improve the running time of their framework, but at the same time guarantee the conservativeness of their results. Finally, the authors present a number of experiments on a large number of benchmarks, which indicate that their approach gives better bounds than a static analysis method.

The article by Quinghui Tang, Sandeep Gupta and Georgios Varsamopoulos presents their work on proposing a general methodology to address thermal effects and constraints in the scheduling of distributed cyber-physical systems. It presents an abstract heat-flow model and shows how to identify and characterize possible thermal interference. The article argues that the energy-related interaction of the distributed cyber-physical system with the environment can be manipulated through the scheduling of the operational tasks of the distributed system. Thus, the article presents how to formulate a scheduling problem based on the thermal interference. This can be utilized to produce an operational schedule that is within some specified thermal constraints. Finally, the article shows how this methodology can be utilized on two very different application domains, namely, an implanted biosensor network and a data center.

The work of Truong Nghiem, George Pappas, Rajeev Alur and Antoine Girard focuses on the implementation of time-triggered controllers for linear systems. In this work, they show techniques for synthesizing code from model-based designs of PID controllers so that the gap between the model and the implementation that arises from errors such as quantization, arithmetic errors, and time delays can be accurately bounded. They demonstrate an application of their techniques to compare different implementations of a controller. Synthesizing code for CPS from models is an important problem. This article makes a significant contribution on this front by directly dealing

with factors such as time delays in invoking a control task due to scheduling policy, quantization, and arithmetic errors.

—Georgios Fainekos
Arizona State University

Eric Goubault
CEA LIST

Franjo Ivančić
Nec Laboratories America

Sriram Sankaranarayanan
University of Colorado Boulder
Guest Editors