Guest Editorial: Special Issue of ACM TECS on the ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE 2017)

This special issue of ACM TECS contains selected papers of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE 2017). MEMOCODE's objective is to bring together researchers and practitioners interested in formal methods and models for system design and development to exchange ideas, research results, and lessons learned. System design covers the design and development of hardware, firmware, middleware, and application software for systems ranging from single embedded devices to highly networked CPS and systems in the Internet of Things (IoT). MEMOCODE emphasizes the importance of formal models and methods in correct system design in all aspects of computer system development. In particular, MEMOCODE focuses on research contributions and formal foundations, engineering methods, tools, and experimental case studies.

MEMOCODE 2017 took place in Vienna (Austria) and was co-located with the conference on Formal Methods in Computer-Aided Design (FMCAD). Among the 48 papers submitted to MEMOCODE 2017, we selected the following six articles for inclusion in this special issue, to show the broad spectrum of MEMOCODE's field of interest, which covers all phases of system design.

- Modeling: “[Stochastic Assume-Guarantee Contracts for Cyber-Physical System Design](#)” by Jiwei Li, Pierluigi Nuzzo, Alberto Sangiovanni-Vincentelli, Yugeng Xi, and Dewei Li presents an assume-guarantee contract framework for the design of cyber-physical systems under probabilistic requirements. System behaviors, assumptions, and guarantees are described by a stochastic signal temporal logic. For certain systems, the approach can check contract compatibility, consistency, and refinement, and can generate a controller to guarantee that a contract is satisfied.
- Verification: “[Mining Missing Assumptions from Counter-Examples](#)” by Guillaume Plassan, Katell Morin-Allory, and Dominique Borrione observes that formal verification of register-transfer level hardware designs often leads to reports of false failures, which frequently stem from under-constrained models. The article presents an approach that extracts missing assumptions from counterexamples, which are then presented by designers to correct their models.
- Testing: “[Model-based, Mutation-driven Test Case Generation via Heuristic-guided Branching](#)” by Andreas Fellner, Willibald Krenn, Thorsten Tarrach, Georg Weissenbacher, and Rupert Schlick introduces an algorithmic framework for parallel heuristic-guided searches for test case generation. Since no single heuristic is able to find all the mutants, the best result is achieved by running multiple heuristics independently and combining their results.
- Synthesis: “[Compositional Dataflow Circuits](#)” by Stephen A. Edwards, Richard Townsend, and Martha A. Kim presents a technique for implementing dataflow networks as compositional hardware circuits. Based on a first abstract dataflow model with unbounded buffers that support data-dependent blocks (mux, demux, and nondeterministic merge), the work

shows how to faithfully implement such networks with bounded buffers and handshaking in a compositional synthesis procedure. Inserting or removing buffers only affects the performance but not the functionality of the generated networks.

- Provable Correctness/Security: “[The Mechanized Marriage of Effects and Monads with Applications to High Assurance Hardware](#)” by Thomas N. Reynolds, Adam Procter, William L. Harrison, and Gerard Allwein presents a core calculus of secure hardware descriptions with its formal semantics, security type system, and mechanization in Coq. This work is the core of the functional HDL ReWire and supports a full-fledged, formal methodology for producing high assurance hardware.
- Quantified Security: “[Quantifying the Information Leakage in Cache Attacks via Symbolic Execution](#)” by Sudipta Chattopadhyay, Moritz Beck, Ahmed Rezine, and Andreas Zeller present the CHALICE framework, which is able to determine, by symbolic simulation, the amount of information that can actually leak through cache timing attacks for a given program, a cache model, and an input. The core of CHALICE is a novel approach to quantify information leaks that can highlight critical cache side-channel leaks on arbitrary binary code.

We are happy the authors of these articles agreed to extend their MEMOCODE papers published in the *Proceedings of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design* to journal publications, which have been subjected to the standard ACM TECS review process. This selection of papers was accepted and is now included in this special issue.

We would like to thank the many people who contributed to the success of this special issue. In particular, we thank the reviewers for their valuable feedback to the authors. We would also like to thank the editor-in-chief, Prof. Sandeep K. Shukla, for suggesting this special issue, and Ms. Laura Lander for her support in the review and publication process.

Patricia Derler, National Instruments
Klaus Schneider, TU Kaiserslautern
Jean-Pierre Talpin, INRIA, Rennes

(Guest Editors and Organizers of MEMOCODE 2017)