Journal of Universal Computer Science, vol. 13, no. 13 (2007), 1970-1971
submitted: 14/12/07, accepted: 21/12/07, appeared: 28/12/07 © J.UCS

Applications of Formal Methods to System Design and Verification

J.UCS Special Issue

Farhad Arbab
CWI, Netherlands
and
Leiden University, Netherlands
Farhad.Arbab@cwi.nl

Marjan Sirjani
University of Tehran, Iran
and
IPM, Iran
msirjani@ut.ac.ir

This special issue contains the extended versions of a selected set of papers presented at the first IPM International Workshop on Foundations of Software Engineering (Theory and Practice), Tehran, Iran, October 1-3, 2005. This event, FSEN05, was organized by the School of Computer Science at the Institute for Studies in Fundamental Sciences (IPM) in Iran, in cooperation with the ACM SIGSOFT.

Shunsuke Sasaki, Tasuku Nishihara, Daisuke Ando, and Masahiro Fujita propose a Hardware/Software co-design and verification methodology based on system dependence graphs. They accept any combination of C/C++/SpecC descriptions as input designs. A system dependence graph shows the dependencies among statements and/or expressions in a design and is used for analyzing and verifying the design, adding parallelism into the designs, and HW/SW partitioning.

Lorenzo Capra and Walter Cazzola propose a framework based on Petri nets for keeping functional aspects separate from evolutionary aspects. The authors propose that with this approach they support adaptability, while they keep the model of a system as simple as possible, and preserve and exploit the ability to formally verify system properties.

Mario Bravetti, Adalberto Casalboni, Manuel Nunez, and Ismael Rodriguez show how to develop suitable designs for e-barter models based on web services using WS-BPEL. An e-barter system is an e-commerce environment where transactions do not necessarily involve money. It is a multi-agent system whose structure reflects a tree of markets and where agents perform exchanges of re-

sources on behalf of their respective users. Starting from formal specifications, the authors show how to develop suitable designs for such systems out of Web services using WS-BPEL. The absence of sufficient practical details in formal specifications presents challenges in this development, and leads to multiple alternative designs that comply with the same set of specifications.

Hossein Hojjat, Hootan Nakhost, and Marjan Sirjani propose a formal proof for the Perlman Spanning Tree Protocol (STP) by integrating module checking and deduction. STP is used in the IEEE 802.1D standard for the Media Access Control layer. For module checking, the authors apply the Rebeca modular verification techniques developed earlier by the last co-author and her group. Through the STP example, they show that these techniques are efficiently applicable in model checking of open systems.

Farhad Arbab
Marjan Sirjani
Amsterdam, December, 2007