Preface

This volume contains the proceedings of the 19th International SPIN Workshop on Model Checking of Software, held at the University of Oxford, during 23–24 July, 2012. The SPIN workshop series is an annual forum for researchers and practitioners interested in verification of software systems. The traditional focus of SPIN has been on explicit-state model checking techniques, as implemented in SPIN and other tools. While such techniques are still of key interest to the workshop, its scope has broadened over recent years to cover techniques for verification and formal testing of software systems in general.

SPIN 2012 features three invited talks, from Tom Ball, Andrey Rybalchenko and Andreas Zeller. Tom Ball (Microsoft Research) is one of the pioneers of practical software verification, especially through his work on the SLAM project. His talk and associated invited paper (co-authored with colleagues at Microsoft Research) provide an overview of recent advances in SMT solving at Microsoft Research related to fixed points, interpolants, automata and polynomials. Andrey Rybalchenko (TU Munich) is an expert in theories, algorithms and tools for improving the quality of software. One of his major interests, and the topic of his SPIN talk, is automatic synthesis of software verification tools. Andreas Zeller (Saarland University) is well known for his work on analysis of large software systems and their development process, particularly through repository mining techniques. His talk at SPIN was on the challenge of modular verification for legacy systems, using mining to discover specifications automatically.

The workshop also featured an invited tutorial from Cristian Cadar (Imperial College London): “How to Crash Your Code Using Dynamic Symbolic Execution.” Cristian is an expert on software testing and bug-finding using dynamic symbolic execution and related techniques, and is one of the authors of the widely used KLEE system. In addition to the tutorial, Cristian contributed an invited paper, “High-Coverage Symbolic Patch Testing,” co-authored with Paul Marinescu.

SPIN 2012 received 30 submissions, from which the Program Committee accepted 11 regular papers and 5 tool demonstration papers. All papers received at least three reviews, with the majority receiving at least four. Program Committee members with conflicts of interest were excluded from all discussions of relevant submissions. The reviewers discussed papers with neither overwhelmingly positive or negative reviews until a consensus was reached. In some of these cases, papers were accepted subject to a shepherding process in which the Chairs ensured that authors revised their papers to incorporate particular changes recommended by reviewers. In all such instances, the authors obliged and the papers were accepted. The editors are extremely grateful to the members of the Program Committee and their subreviewers for working under a tight
deadline, and to the authors of the accepted papers for the quick turnaround in producing camera-ready copies.

We are indebted to the members of the SPIN Steering Committee, especially Gerard Holzmann and Stefan Leue, and the Chairs of SPIN 2011, Alex Groce and Madanlal Musuvathi, for their advice related to the organization of this workshop. Thanks also to Gerard Holzmann for designing this year’s workshop poster. We are also very grateful to Elizabeth Walsh at the University of Oxford for invaluable assistance with local organization. The submission, review and revision processes, as well as the collation of the workshop proceedings, were all supported by the EasyChair conference management system; we are extremely grateful to the authors and maintainers of EasyChair for this free service. Finally, we offer our sincere thanks to ARM, Codeplay, Microsoft Research and Monoidics, who generously provided financial support to SPIN 2012.

July 2012

Alastair Donaldson

David Parker
Organization

Steering Committee

Dragan Bošnački  Eindhoven University of Technology, The Netherlands
Susanne Graf  CNRS/VERIMAG, France
Gerard Holzmann  NASA/JPL, USA
Stefan Leue  University of Konstanz, Germany
Willem Visser  University of Stellenbosch, South Africa

Program Chairs

Alastair Donaldson  Imperial College London, UK
David Parker  University of Birmingham, UK

Local Organization

Michael Tautschnig  University of Oxford, UK

Program Committee

Christel Baier  University of Dresden, Germany
Dirk Beyer  University of Passau, Germany
Dragan Bošnački  Eindhoven University of Technology, The Netherlands
Alastair Donaldson  Imperial College London, UK
Stefan Edelkamp  TZI University Bremen, Germany
Alex Groce  Oregon State University, USA
Gerard Holzmann  NASA/JPL, USA
Radu Iosif  VERIMAG, CNRS, France
Stefan Leue  University of Konstanz, Germany
Eric Mercer  Brigham Young University, USA
Alice Miller  University of Glasgow, UK
Madanlal Musuvathi  Microsoft Research, Redmond, USA
David Parker  University of Birmingham, UK
Corina Pasareanu  NASA Ames, USA
Doron Peled  Bar Ilan University, Israel
Jaco van de Pol  University of Twente, The Netherlands
Kees Pronk  Delft University of Technology, The Netherlands
Shaz Qadeer  Microsoft Research, Redmond, USA
VIII Organization

Alastair Reid ARM, UK
Tayssir Touili LIAFA, CNRS, France
Helmut Veith Vienna University of Technology, Austria
Thomas Wahl Northeastern University, USA

Subreviewers

Amin Alipour Florian Leitner-Fischer Mitra Tabaei Befrouei
Adrian Beer Carl Leonardsson Mark Timmer
Axel Belinfante Stefan Löwe Oksana Tkachuk
Annu John Hugo Daniel Macedo Philipp Wendler
Gijs Kant Kristin Yvonne Rozier Anton Wijs
Filip Konecny Philipp Ruemmer Chaoqiang Zhang
Igor Konnov Jiri Simacek Florian Zuleger
Alfons Laarman Fu Song

Sponsors

ARM Ltd. Codeplay Software Ltd.
Microsoft Research Monoidics Ltd.
Table of Contents

Invited Contributions

Beyond First-Order Satisfaction: Fixed Points, Interpolants, Automata and Polynomials .................................................. 1
Thomas Ball, Nikolaj Bjørner, Leonardo de Moura, Kenneth L. McMillan, and Margus Veanes

High-Coverage Symbolic Patch Testing ........................................ 7
Paul Dan Marinescu and Cristian Cadar

Towards Automatic Synthesis of Software Verification Tools .......... 22
Andrey Rybalchenko

Mining Models ........................................................................... 23
Andreas Zeller

Model Checking Techniques

Counterexample Explanation by Anomaly Detection ....................... 24
Stefan Leue and Mitra Tabaei Befrouei

Combining the Sweep-Line Method with the Use of an External-Memory Priority Queue ......................................................... 43
Sami Evangelista and Lars Michael Kristensen

A Compositional Minimization Approach for Large Asynchronous Design Verification ......................................................... 62
Hao Zheng, Emmanuel Rodriguez, Yingying Zhang, and Chris Myers

Parallel Model Checking 1

On Parallel Software Verification Using Boolean Equation Systems ...... 80
Alexander Ditter, Milan Češka, and Gerald Lüttgen

Improving GPU Sparse Matrix-Vector Multiplication for Probabilistic Model Checking ......................................................... 98
Anton J. Wijs and Dragan Bošnački

Case Studies

Gossiping Girls Are All Alike .................................................... 117
Theo C. Ruys and Pim Kars
Formal Verification of Hierarchically Distributed Agent Based Protection Scheme in Smart Grid ........................................ 137
  Shravan Garlapati and Sandeep K. Shukla

Parallel Model Checking 2
Parallelizing the Spin Model Checker ........................................ 155
  Gerard J. Holzmann
Parallel Model Checking Using Abstraction ...................................... 172
  Ethan Burns and Rong Zhou

Model Checking for Concurrency
McPatom: A Predictive Analysis Tool for Atomicity Violation Using Model Checking .................................................. 191
  Reng Zeng, Zhuo Sun, Su Liu, and Xudong He
Parameterized Model Checking of Fine Grained Concurrency ............ 208
  Divijot Sethi, Muralidhar Talupur, Daniel Schwartz-Narbonne, and Sharad Malik

Tool Demonstrations
mctau: Bridging the Gap between Modest and UPPAAL ............... 227
  Jonathan Bogdoll, Alexandre David, Arnd Hartmanns, and Holger Hermanns
  Heinz Riener and Görschwin Fey
Model Checking DSL-Generated C Source Code ............................ 241
  Martin Sulzmann and Axel Zechner
SMTInterpol: An Interpolating SMT Solver .................................. 248
  Jürgen Christ, Jochen Hoenicke, and Alexander Nutz
S2N: Model Transformation from SPIN to NuSMV (Tool Paper) ....... 255
  Yong Jiang and Zongyan Qiu

Author Index .......................................................................... 261