

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Catherine Dubois (Ed.)

Tests and Proofs

Third International Conference, TAP 2009
Zurich, Switzerland, July 2-3, 2009
Proceedings

Volume Editor

Catherine Dubois
ENSIIE-CÉDRIC

1 square de la résistance, 91025 Évry Cedex, France
E-mail: dubois@ensiie.fr

Library of Congress Control Number: 2009929546

CR Subject Classification (1998): D.2.4-5, F.3, D.4, C.4, K.4.4, C.2

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-642-02948-5 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-02948-6 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12717774 06/3180 5 4 3 2 1 0

Preface

This volume¹ contains the research papers and invited papers presented at the Third International Conference on Tests and Proofs (TAP 2009) held at ETH Zurich, Switzerland, during July 2–3, 2009.

The TAP conference is devoted to the convergence of proofs and tests. It combines ideas from both sides for the advancement of software quality. To prove the correctness of a program is to demonstrate, through impeccable mathematical techniques, that it has no bugs; to test a program is to run it with the expectation of discovering bugs. The two techniques seem contradictory: if you have proved your program, it is fruitless to comb it for bugs; and if you are testing it, that is surely a sign that you have given up on any hope of proving its correctness. Accordingly, proofs and tests have, since the onset of software engineering research, been pursued by distinct communities using rather different techniques and tools. And yet the development of both approaches leads to the discovery of common issues and to the realization that each may need the other. The emergence of model checking has been one of the first signs that contradiction may yield to complementarity, but in the past few years an increasing number of research efforts have encountered the need for combining proofs and tests, dropping earlier dogmatic views of incompatibility and taking instead the best of what each of these software engineering domains has to offer.

The first TAP conference (held at ETH Zurich in February 2007) was an attempt to provide a forum for the cross-fertilization of ideas and approaches from the testing and proving communities. The 2008 edition took place in the Monash University Prato Centre near Florence. For the third TAP conference we came back to ETH Zurich. This third edition was co-located with other software conferences, in particular TOOLS Europe.

We wish to sincerely thank all the authors who submitted their work for consideration. We would also like to thank the Program Committee members as well as the additional referees for their great effort and work of high quality in the review and selection process. Their names are listed on the following pages.

There were 20 submissions. Each submission was reviewed by at least three persons. The Committee decided to accept ten research papers. The program also included two keynote talks. We are grateful to Sriram Rajamani (Microsoft Research, India) and Boutheina Chetali (Gemalto, France) for accepting the invitation to address the conference.

The conference also included some short presentations that were reviewed by at least one Program Committee member. They are not included in this proceedings volume but are part of a technical ETH report entitled *TAP 2009: short papers*.

¹ This volume was prepared with EasyChair. Many thanks to its developer.

The success of the conference resulted from a team effort. We are grateful to the Conference Chair and the Steering Committee members for their support at every stage in the conference preparation. We also thank all the members of the Organizing Committee, in particular Yi Wei and Stephan van Staden, ETH Zurich. Finally, we gratefully acknowledge the material and financial support provided by the Chair of Software Engineering, ETH Zurich.

May 2009

Catherine Dubois

Conference Organization

Conference Chair

Bertrand Meyer ETH Zurich, Switzerland

Program Chair

Catherine Dubois ENSIIE, France

Program Committee

Bernhard Aichernig	TU Graz, Austria
Bernhard Beckert	University of Koblenz, Germany
Patrice Chalin	Concordia University, Canada
Yoonsik Cheon	University of Texas at El Paso, USA
Koen Claessen	Chalmers University of Technology, Sweden
Gilles Dowek	École Polytechnique, France
Angelo Gargantini	University of Bergamo, Italy
Arnaud Gotlieb	IRISA, France
Yuri Gurevich	Microsoft Research, USA
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Reiner Hähnle	Chalmers University of Technology, Sweden
Ewen Maclean	Heriot-Watt University, UK
Karl Meinke	KTH Royal Institute of Technology, Sweden
Sam Owre	SRI International, USA
Wolfram Schulte	Microsoft Research, USA
Mark Utting	Waikato University, New Zealand

Additional Reviewers

Bernard Botella	Richard Bubel	Andrea Calvagna
Bruno Dutertre	Frédéric Gervais	Christoph Gladisch
K. Rustan M. Leino	Patricia Mouy	Ulf Norell
David Pichardie	Vlad Rusu	Natarajan Shankar
David Streader	Ashish Tiwari	Margus Veanes
Burkhart Wolff		

Steering Committee

Yuri Gurevich	Microsoft Research, USA
Bertrand Meyer	ETH Zurich, Switzerland

Local Organization

Yi Wei	ETH Zurich, Switzerland
Stephan van Staden	ETH Zurich, Switzerland
Claudia Günthart	ETH Zurich, Switzerland

Sponsoring Institutions

Chair of Software Engineering, ETH Zurich, Switzerland
ENSIIE, Évry, France

Table of Contents

Security Testing and Formal Methods for High Levels Certification of Smart Cards	1
<i>Boutheina Chetali</i>	
Verification, Testing and Statistics	6
<i>Aditya Nori and Sriram K. Rajamani</i>	
Development of a Generic Voter under FoCaL	10
<i>Philippe Ayrault, Thérèse Hardin, and François Pessaux</i>	
Combining Satisfiability Solving and Heuristics to Constrained Combinatorial Interaction Testing	27
<i>Andrea Calvagna and Angelo Gargantini</i>	
Incorporating Historical Test Case Performance Data and Resource Constraints into Test Case Prioritization	43
<i>Yalda Fazlalizadeh, Alireza Khalilian, Mohammad Abdollahi Azgomi, and Saeed Parsa</i>	
Complementary Criteria for Testing Temporal Logic Properties	58
<i>Gordon Fraser and Franz Wotawa</i>	
Could We Have Chosen a Better Loop Invariant or Method Contract?	74
<i>Christoph Gladisch</i>	
Consistency, Independence and Consequences in UML and OCL Models	90
<i>Martin Gogolla, Mirco Kuhlmann, and Lars Hamann</i>	
Dynamic Symbolic Execution for Testing Distributed Objects	105
<i>Andreas Griesmayer, Bernhard Aichernig, Einar Broch Johnsen, and Rudolf Schlatte</i>	
Combining Model Checking and Testing in a Continuous HW/SW Co-verification Process	121
<i>Paula Herber, Florian Friedemann, and Sabine Glesner</i>	
Symbolic Execution Based Model Checking of Open Systems with Unbounded Variables	137
<i>Nicolas Rapin</i>	

Finding Errors of Hybrid Systems by Optimising an Abstraction-Based
Quality Estimate 153
 Stefan Ratschan and Jan-Georg Smaus

Author Index 169