Lecture Notes in Computer Science 2772
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Nachum Dershowitz (Ed.)

Verification: Theory and Practice

Essays Dedicated to Zohar Manna
on the Occasion of His 64th Birthday

Springer

Volume Editor

Nachum Dershowitz
Tel Aviv University, School of Computer Science
Ramat Aviv, Tel Aviv 69978, Israel
E-mail: nachumd@cs.tau.ac.il

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): F.3, D.2, D.3, F.4, F.1, C.3, C.2.4, I.2.3

ISSN 0302-9743
ISBN 3-540-21002-4 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10931370 06/3142 5 4 3 2 1 0

והמשכלים יזהרו כזהר הרקיע

—Daniel 12:3

ZOHAR MANNA (b. 1939)

Preface

Zohar Manna, founding father of the study and application of formal methods for software and hardware verification, turned 64 early this (Gregorian) year, a date of numerological significance to cognoscenti in the realm of binary computers.[1] To honor this event, many of Zohar's graduate students, research collaborators, and computer-science colleagues gathered in Sicily for a symposium on subjects related to Zohar's manifold contributions in the field. Their breadth and depth were a tribute to Zohar's lasting impact on the field.

The symposium was held in Taormina, Sicily, Italy between June 29 and July 4, 2003. Local arrangements were coordinated by Alfredo Ferro of Catania University. The help of Ugo Montanari was instrumental in the success of the event and is most gratefully acknowledged. Thanks are also due Domenico Cantone, Rajeev Alur, the late Armando Haeberer, Tom Henzinger, Paola Schettino, and Henny Sipma. The meeting received generous support from the following institutions:

- Dipartimento di Informatica of the University of Pisa;
- School of Computer Science of Tel Aviv University;
- Lipari International School for Computer Science Researchers; and
- Dipartimento di Matematica e Informatica of Catania University.

The event comprised the following lectures:

1. Amir Pnueli: "TLPVS: a PVS-Based LTL Verification System" (with Tamarah Arons)
2. Bernd Finkbeiner: "Runtime Verification with Alternating Automata" (with Sriram Sankaranarayanan and Henny Sipma)
3. Rajeev Alur: "Formal Analysis of Hierarchical State Machines"
4. Luca de Alfaro: "Games and Mu-Calculus"
5. Manfred Broy: "A Functional Calculus for Specification and Verification of Nondeterministic Interactive Systems"
6. Martín Abadi: "Verification of Security Protocols: Certified Email in the Applied Pi Calculus"
7. Egon Börger: "The ASM Ground Model Method as a Foundation for Requirements Engineering"

[1] The choice of the $1{,}000{,}000_2$-th birthday in computer circles dates back at least to the honoring of John McCarthy's birthday in 1991, conceived by Don Knuth and Jeff Ullman. It is also the subject of the famous Beatles number, "When I'm Sixty-Four," by John Lennon and Paul McCartney, recorded in 1966, but composed earlier.

8. Willem-Paul de Roever: "A Compositional Operational Semantics for Java_{MT}" (with Erika Ábrahám, Frank S. de Boer, and Martin Steffen)
9. Peter Pepper: "Colimits for Concurrent Collectors" (with Dusko Pavlovic and Doug Smith)
10. Ugo Montanari: "A Formal Basis for Reasoning on Programmable QoS" (with Rocco De Nicola, Gianluigi Ferrari, Rosario Pugliese, and Emilio Tuosto)
11. Thomas Henzinger: "Extreme Model Checking" (with Ranjit Jhala, Rupak Majumdar, and Marco A.A. Sanvido)
12. Shmuel Katz: "Aspect Validation Using Model Checking" (with Marcelo Sihman)
13. Alberto Policriti: "Binary Extensions of S1S and the Composition Method" (with Enrico Marzano and Angelo Montanari)
14. Ashok Chandra: "On the Semantics of 'Unstructured' Data"
15. Gérard Huet: "Mixed Automata"
16. Jean-Louis Lassez: "Qualitative Theorem Proving in Linear Constraints" (with Vijay Chandru)
17. Hubert Comon-Lundh: "Easy Intruder Deductions" (with Ralf Treinen)
18. Patrick Cousot: "Verification by Abstract Interpretation"
19. Alfredo Ferro: "Efficient Boundary Values Generation in General Metric Spaces for Software Component Testing" (with Rosalba Giugno and Alfredo Pulvirenti)
20. Jean Vuillemin: "Digital Algebra and Circuits"
21. Dines Bjørner: "Domain Engineering: a 'Radical Innovation' for Software and Systems Engineering?"
22. Domenico Cantone: "Notes from the Logbook of a Proof-Checker's Project" (with Eugenio G. Omodeo, Jacob T. Schwartz, and Pietro Ursino)
23. Krishna Palem: "Verification and Proof as Experiment Mathematical Truth from a Thermodynamic Perspective"
24. Tom Maibaum: "Some Institutional Requirements for Temporal Reasoning on Dynamic Reconfiguration of Component-Based Systems" (with Nazareno Aguirre)
25. Ben Moszkowski: "A Hierarchical Completeness Proof for Propositional Temporal Logic"
26. Nachum Dershowitz: "Bounded Fairness" (with D.N. Jayasimha and Seungjoon Park)

The 32 invited chapters of this volume more or less represent the proceedings of that event. A few lectures are not represented; some varied somewhat from the subsequent written contributions; and some contributors to this volume were unfortunately unable to attend the event.

A one-day symposium in Zohar's honor was also held at Tel Aviv University on Friday, May 16, 2003, at which the following talks were presented:

1. Haim Wolfson, "Welcome"
2. Adi Shamir, "The Security of Smart Cards"
3. Amos Fiat, "Thwarting Traffic Analysis: Obscurant Networks for Provable Anonymity"
4. Orna Grumberg, "The Abstraction-Refinement Framework in Model Checking"
5. David Harel, "Some Analogues of Partial and Total Correctness in Scenario-Based Programming"
6. Danny Dolev, "Asynchronous Resource Discovery"
7. Yaacov Choueka, "Theory of Automata on Infinite Structures: the Early History. Memories and Reminiscences"
8. Nachum Dershowitz, "Closing Remarks"
9. Zohar Manna, "Response"

Ramat Aviv
US Thanksgiving 2003
2 Kislev 5764 Nachum Dershowitz

Table of Contents

Frontispiece: Zohar Manna

Technical Papers