Rajeev Alur
Doron A. Peled (Eds.)

LNCS 3114

Computer Aided Verification

16th International Conference, CAV 2004
Boston, MA, USA, July 2004
Proceedings

Springer

Rajeev Alur Doron A. Peled (Eds.)

Computer Aided Verification

16th International Conference, CAV 2004
Boston, MA, USA, July 13-17, 2004
Proceedings

Springer

Volume Editors

Rajeev Alur
University of Pensylvania, Department of Computer und Information Science
3330 Walnut Street, Philadelphia, PA 19104, USA
E-mail: alur@cis.upenn.edu

Doron A. Peled
University of Warwick, Department of Computer Science
Coventry, CV4 7AL, UK
E-mail: pdoron@dcs.warwick.ac.uk

Library of Congress Control Number: 2004108215

CR Subject Classification (1998): F.3, D.2.4, D.2.2, F.4.1, I.2.3, B.7.2, C.3

ISSN 0302-9743
ISBN 3-540-22342-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11015802 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3114

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Preface

This volume contains the proceedings of the conference on *Computer Aided Verification*, CAV 2004, held in Boston, Massachusetts, USA, July 13–17, 2004. CAV 2004 was the 16th in a series of conferences dedicated to the advancement of the theory and practice of computer-assisted formal analysis methods for software and hardware systems. The conference covers the spectrum from theoretical results to concrete applications, with an emphasis on practical verification tools and the algorithms and techniques that are needed for their implementation. The conference has traditionally drawn participation from researchers as well as practitioners in both academia and industry.

CAV 2004 was colocated with the ACM International Symposium on Software Testing and Analysis (ISSTA 2004), and was partially sponsored by the ACM SIGSOFT. The colocation reflects the increasing synergy between research on verification and testing, and emerging applications of formal verification to software analysis. Joint CAV-ISSTA events included a distinguished plenary lecture by David Harel and a special session exploring various approaches to the specification and verification of concurrent software organized by Shaz Qadeer. The program of the conference consisted of 32 regular papers and 16 tool papers, selected from a total of 144 submissions. The conference was preceded by a tutorial on processor verification, on July 12, 2004, with three invited lectures by Randal E. Bryant, David L. Dill and Warren A. Hunt, Jr. The conference also included invited talks by Mary Jean Harrold and Thomas W. Reps. Two workshops were associated with CAV 2004:

- BMC 2004: Second International Workshop on Bounded Model Checking
- GDV 2004: Games in Design and Verification

We would like to thank all the program committee members and the subreferees for their excellent work in evaluating the submissions and the selection of the program. Our thanks also go to the steering committee members and the organizers of CAV 2003 for their helpful advice. Special thanks go to George Avrunin, the ISSTA General Chair, and Erin Dolan of ACM, for their help with the local organization. We would like to acknowledge the generous sponsorship of Cadence Design Systems, IBM Research, Intel Research, Microsoft Research and the John Von Neumann Minerva Center for Verification of Reactive Systems. Their support helped us reduce the registration fee for the graduate students.

The CAV community is deeply saddened by the sudden demise of Dr. Rob T. Gerth. Rob was a highly regarded researcher with many notable contributions to the theory and practice of formal verification. For CAV 2004, we had invited Rob to join the program committee as well as to give a tutorial on processor verification. This LNCS volume containing the CAV 2004 proceedings is dedicated to Rob, and includes a special presentation, commemorating his scientific accomplishments and collaborations.

May 2004 Rajeev Alur and Doron A. Peled

Program Committee

Rajeev Alur (University of Pennsylvania, USA, co-chair)
David Basin (ETH Zurich, Switzerland)
Armin Biere (ETH Zurich, Switzerland)
Dennis Dams (Bell Labs, Lucent Technologies, USA)
David L. Dill (Stanford University, USA)
E. Allen Emerson (University of Texas at Austin, USA)
Kousha Etessami (University of Edinburgh, UK)
Steven German (IBM Research, USA)
Mike Gordon (University of Cambridge, UK)
Aarti Gupta (NEC Labs America, USA)
Klaus Havelund (NASA Ames, USA)
Holger Hermanns (Saarland University, Germany)
Alan Hu (University of British Columbia, Canada)
Bengt Jonsson (Uppsala University, Sweden)
Andreas Kuehlman (Cadence Berkeley Labs, USA)
Salvatore La Torre (University of Salerno, Italy)
Oded Maler (Verimag, France)
Pete Manolios (Georgia Institute of Technology, USA)
Ken McMillan (Cadence Berkeley Labs, USA)
Anca Muscholl (University of Paris 7, France)
Chris Myers (University of Utah, USA)
Doron Peled (University of Warwick, UK, co-chair)
Fabio Somenzi (University of Colorado at Boulder, USA)
Amir Pnueli (New York University, USA)
Shaz Qadeer (Microsoft Research, USA)
Jun Sawada (IBM Research, USA)
Frits Vaandrager (University of Nijmegen, The Netherlands)
Pierre Wolper (University of Liege, Belgium)
Sergio Yovine (Verimag, France)

Steering Committee

Edmund M. Clarke (Carnegie Mellon University, USA)
Robert P. Kurshan (Cadence, USA)
Amir Pnueli (New York University, USA)
Mike Gordon (University of Cambridge, UK)

Referees

Parosh Abdulla
Nina Amla
Suzana Andova
Tamarah Arons
Cyrille Artho
Eugene Asarin
Christel Baier
Ittai Balaban
Howard Barringer

Jason Baumgartner
Bernd Becker
Michael Benedikt
Saddek Bensalem
Sergey Berezin
Mikhail Bernadsky
Jesse Bingham
Roderick Bloem
Johan Blom
Bernard Boigelot
Dragan Bosnacki
Ahmed Bouajjani
Marius Bozga
Tevfik Bultan
Donald Chai
Jacob Chang
Marsha Chechik
Ling Cheung
Alessandro Cimatti
Scott Cotton
Thao Dang
Conrado Daws
Johann Deneux
Jyotirmoy Deshmukh
Peter Dillinger
Xiaoqun Du
Elena Dubrova
Avijit Dutta
Marco Faella
Manuel Fahndrich
Ansgar Fehnker
Xiushan Feng
David Fink
Bernd Finkbeiner
Carsten Fritz
Marc Geilen
Blaise Genest
Philippe Gerner
Alain Girault
Amit Goel
Gregor Goessler
Peter Habermehl
Malek Haroud
John Hatcliff
Marc Herbstritt
Gerard Holzmann
Jozef Hooman
Michael Huth
Franjo Ivancic
Paul Jackson
Sadegh Jahanpour
Petr Jancar
Geert Janssen
Bertrand Jeannet
Sven Johr
Rajeev Joshi
Vineet Kahlon
Huthasana Kalyanam
Joost-Pieter Katoen
Nathan Kitchen
Felix Klaedtke
Nils Klarlund
Christos Kloukinas
Matthias Kuntz
Orna Kupferman
Shuvendu Lahiri
Yassine Lakhnech
Frederic Lang
Ruggiero Lanotte
Joyce Lauer
Ranko Lazic
Axel Legay
Martin Leucker
Bing Li
Scott Little
Rupak Majumdar
Shawn Manley
Heiko Mantel
Marco Maratea
Eric Mercer
Markus Mueller-Olm
Aniello Murano
Madan Musuvathi
David N. Jansen
Kedar Namjoshi
Margherita Napoli
Kelvin Ng
Dejan Nickovic
Marcus Nilsson
Iulian Ober
Alfredo Olivero
Joel Ouaknine
Domenico Parente
Gennaro Parlato
Viresh Paruthi
Corina Pasareanu
Mark Pichora
Nir Piterman
Andreas Podelski
Ramanujam
Kavita Ravi
Theo Ruys
Gerardo Schneider
Viktor Schuppan
Sanjit Seshia
Ilya Shlyakhter
Eric Smith
Oleg Sokolsky
Sudarshan Srinivasan
Ian Stark
Martin Steffen
Colin Stirling
Marielle Stoelinga
Val Tannen
P.S. Thiagarajan
Tayssir Touili
Richard Trefler
Stavros Tripakis
Yaroslav Usenko
Antti Valmari
Helmut Veith
Miroslav Velev
Willem Visser
Daron Vroon
Thomas Wahl
David Walter
Thomas Wilke
Aleksander Zaks
Yunshan Zhu
Lenore Zuck
Rob van Glabbeek

Lecture Notes in Computer Science

For information about Vols. 1–3015

please contact your bookseller or Springer-Verlag

Vol. 3125: D. Kozen (Ed.), Mathematics of Program Construction. X, 401 pages. 2004.

Vol. 3120: J. Shawe-Taylor, Y. Singer (Eds.), Learning Theory. X, 648 pages. 2004.

Vol. 3114: R. Alur, D.A. Peled (Eds.), Computer Aided Verification. XII, 536 pages. 2004.

Vol. 3112: H. Williams, L. MacKinnon (Eds.), New Horizons in Information Management. XII, 265 pages. 2004.

Vol. 3111: T. Hagerup, J. Katajainen (Eds.), Algorithm Theory - SWAT 2004. XI, 506 pages. 2004.

Vol. 3109: S.C. Sahinalp, S. Muthukrishnan, U. Dogrusoz (Eds.), Combinatorial Pattern Matching. XII, 486 pages. 2004.

Vol. 3105: S. Göbel, U. Spierling, A. Hoffmann, I. Iurgel, O. Schneider, J. Dechau, A. Feix (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. XVI, 304 pages. 2004.

Vol. 3104: R. Kralovic, O. Sykora (Eds.), Structural Information and Communication Complexity. X, 303 pages. 2004.

Vol. 3103: K. Deb (Ed.), Genetic and Evolutionary Computation - GECCO 2004. XLIX, 1439 pages. 2004.

Vol. 3102: K. Deb (Ed.), Genetic and Evolutionary Computation - GECCO 2004. L, 1445 pages. 2004.

Vol. 3101: M. Masoodian, S. Jones, B. Rogers (Eds.), Computer Human Interaction. XIV, 694 pages. 2004.

Vol. 3099: J. Cortadella, W. Reisig (Eds.), Applications and Theory of Petri Nets 2004. XI, 505 pages. 2004.

Vol. 3098: J. Desel, W. Reisig, G. Rozenberg (Eds.), Lectures on Concurrency and Petri Nets. VIII, 849 pages. 2004.

Vol. 3097: D. Basin, M. Rusinowitch (Eds.), Automated Reasoning. XII, 493 pages. 2004. (Subseries LNAI).

Vol. 3096: G. Melnik, H. Holz (Eds.), Advances in Learning Software Organizations. X, 173 pages. 2004.

Vol. 3094: A. Nürnberger, M. Detyniecki (Eds.), Adaptive Multimedia Retrieval. VIII, 229 pages. 2004.

Vol. 3093: S.K. Katsikas, S. Gritzalis, J. Lopez (Eds.), Public Key Infrastructure. XIII, 380 pages. 2004.

Vol. 3092: J. Eckstein, H. Baumeister (Eds.), Extreme Programming and Agile Processes in Software Engineering. XVI, 358 pages. 2004.

Vol. 3091: V. van Oostrom (Ed.), Rewriting Techniques and Applications. X, 313 pages. 2004.

Vol. 3089: M. Jakobsson, M. Yung, J. Zhou (Eds.), Applied Cryptography and Network Security. XIV, 510 pages. 2004.

Vol. 3086: M. Odersky (Ed.), ECOOP 2004 – Object-Oriented Programming. XIII, 611 pages. 2004.

Vol. 3085: S. Berardi, M. Coppo, F. Damiani (Eds.), Types for Proofs and Programs. X, 409 pages. 2004.

Vol. 3084: A. Persson, J. Stirna (Eds.), Advanced Information Systems Engineering. XIV, 596 pages. 2004.

Vol. 3083: W. Emmerich, A.L. Wolf (Eds.), Component Deployment. X, 249 pages. 2004.

Vol. 3080: J. Desel, B. Pernici, M. Weske (Eds.), Business Process Management. X, 307 pages. 2004.

Vol. 3079: Z. Mammeri, P. Lorenz (Eds.), High Speed Networks and Multimedia Communications. XVIII, 1103 pages. 2004.

Vol. 3078: S. Cotin, D.N. Metaxas (Eds.), Medical Simulation. XVI, 296 pages. 2004.

Vol. 3077: F. Roli, J. Kittler, T. Windeatt (Eds.), Multiple Classifier Systems. XII, 386 pages. 2004.

Vol. 3076: D. Buell (Ed.), Algorithmic Number Theory. XI, 451 pages. 2004.

Vol. 3074: B. Kuijpers, P. Revesz (Eds.), Constraint Databases and Applications. XII, 181 pages. 2004.

Vol. 3073: H. Chen, R. Moore, D.D. Zeng, J. Leavitt (Eds.), Intelligence and Security Informatics. XV, 536 pages. 2004.

Vol. 3072: D. Zhang, A.K. Jain (Eds.), Biometric Authentication. XVII, 800 pages. 2004.

Vol. 3070: L. Rutkowski, J. Siekmann, R. Tadeusiewicz, L.A. Zadeh (Eds.), Artificial Intelligence and Soft Computing - ICAISC 2004. XXV, 1208 pages. 2004. (Subseries LNAI).

Vol. 3068: E. André, L. Dybkj{\}ae r, W. Minker, P. Heisterkamp (Eds.), Affective Dialogue Systems. XII, 324 pages. 2004. (Subseries LNAI).

Vol. 3067: M. Dastani, J. Dix, A. El Fallah-Seghrouchni (Eds.), Programming Multi-Agent Systems. X, 221 pages. 2004. (Subseries LNAI).

Vol. 3066: S. Tsumoto, R. S lowiński, J. Komorowski, J.W. Grzymala-Busse (Eds.), Rough Sets and Current Trends in Computing. XX, 853 pages. 2004. (Subseries LNAI).

Vol. 3065: A. Lomuscio, D. Nute (Eds.), Deontic Logic in Computer Science. X, 275 pages. 2004. (Subseries LNAI).

Vol. 3064: D. Bienstock, G. Nemhauser (Eds.), Integer Programming and Combinatorial Optimization. XI, 445 pages. 2004.

Vol. 3063: A. Llamosí, A. Strohmeier (Eds.), Reliable Software Technologies - Ada-Europe 2004. XIII, 333 pages. 2004.

Vol. 3062: J.L. Pfaltz, M. Nagl, B. Böhlen (Eds.), Applications of Graph Transformations with Industrial Relevance. XV, 500 pages. 2004.

Vol. 3061: F.F. Ramas, H. Unger, V. Larios (Eds.), Advanced Distributed Systems. VIII, 285 pages. 2004.

Vol. 3060: A.Y. Tawfik, S.D. Goodwin (Eds.), Advances in Artificial Intelligence. XIII, 582 pages. 2004. (Subseries LNAI).

Vol. 3059: C.C. Ribeiro, S.L. Martins (Eds.), Experimental and Efficient Algorithms. X, 586 pages. 2004.

Vol. 3058: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 233 pages. 2004.

Vol. 3057: B. Jayaraman (Ed.), Practical Aspects of Declarative Languages. VIII, 255 pages. 2004.

Vol. 3056: H. Dai, R. Srikant, C. Zhang (Eds.), Advances in Knowledge Discovery and Data Mining. XIX, 713 pages. 2004. (Subseries LNAI).

Vol. 3055: H. Christiansen, M.-S. Hacid, T. Andreasen, H.L. Larsen (Eds.), Flexible Query Answering Systems. X, 500 pages. 2004. (Subseries LNAI).

Vol. 3054: I. Crnkovic, J.A. Stafford, H.W. Schmidt, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 311 pages. 2004.

Vol. 3053: C. Bussler, J. Davies, D. Fensel, R. Studer (Eds.), The Semantic Web: Research and Applications. XIII, 490 pages. 2004.

Vol. 3052: W. Zimmermann, B. Thalheim (Eds.), Abstract State Machines 2004. Advances in Theory and Practice. XII, 235 pages. 2004.

Vol. 3051: R. Berghammer, B. Möller, G. Struth (Eds.), Relational and Kleene-Algebraic Methods in Computer Science. X, 279 pages. 2004.

Vol. 3050: J. Domingo-Ferrer, V. Torra (Eds.), Privacy in Statistical Databases. IX, 367 pages. 2004.

Vol. 3049: M. Bruynooghe, K.-K. Lau (Eds.), Program Development in Computational Logic. VIII, 539 pages. 2004.

Vol. 3047: F. Oquendo, B. Warboys, R. Morrison (Eds.), Software Architecture. X, 279 pages. 2004.

Vol. 3046: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1016 pages. 2004.

Vol. 3045: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1040 pages. 2004.

Vol. 3044: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1140 pages. 2004.

Vol. 3043: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1180 pages. 2004.

Vol. 3042: N. Mitrou, K. Kontovasilis, G.N. Rouskas, I. Iliadis, L. Merakos (Eds.), NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. XXXIII, 1519 pages. 2004.

Vol. 3040: R. Conejo, M. Urretavizcaya, J.-L. Pérez-de-la-Cruz (Eds.), Current Topics in Artificial Intelligence. XIV, 689 pages. 2004. (Subseries LNAI).

Vol. 3039: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1271 pages. 2004.

Vol. 3038: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1311 pages. 2004.

Vol. 3037: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 745 pages. 2004.

Vol. 3036: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 713 pages. 2004.

Vol. 3035: M.A. Wimmer (Ed.), Knowledge Management in Electronic Government. XII, 326 pages. 2004. (Subseries LNAI).

Vol. 3034: J. Favela, E. Menasalvas, E. Chávez (Eds.), Advances in Web Intelligence. XIII, 227 pages. 2004. (Subseries LNAI).

Vol. 3033: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVIII, 1076 pages. 2004.

Vol. 3032: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVII, 1112 pages. 2004.

Vol. 3031: A. Butz, A. Krüger, P. Olivier (Eds.), Smart Graphics. X, 165 pages. 2004.

Vol. 3030: P. Giorgini, B. Henderson-Sellers, M. Winikoff (Eds.), Agent-Oriented Information Systems. XIV, 207 pages. 2004. (Subseries LNAI).

Vol. 3029: B. Orchard, C. Yang, M. Ali (Eds.), Innovations in Applied Artificial Intelligence. XXI, 1272 pages. 2004. (Subseries LNAI).

Vol. 3028: D. Neuenschwander, Probabilistic and Statistical Methods in Cryptology. X, 158 pages. 2004.

Vol. 3027: C. Cachin, J. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT 2004. XI, 628 pages. 2004.

Vol. 3026: C. Ramamoorthy, R. Lee, K.W. Lee (Eds.), Software Engineering Research and Applications. XV, 377 pages. 2004.

Vol. 3025: G.A. Vouros, T. Panayiotopoulos (Eds.), Methods and Applications of Artificial Intelligence. XV, 546 pages. 2004. (Subseries LNAI).

Vol. 3024: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 621 pages. 2004.

Vol. 3023: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 611 pages. 2004.

Vol. 3022: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 621 pages. 2004.

Vol. 3021: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 633 pages. 2004.

Vol. 3019: R. Wyrzykowski, J.J. Dongarra, M. Paprzycki, J. Wasniewski (Eds.), Parallel Processing and Applied Mathematics. XIX, 1174 pages. 2004.

Vol. 3018: M. Bruynooghe (Ed.), Logic Based Program Synthesis and Transformation. X, 233 pages. 2004.

Vol. 3017: B. Roy, W. Meier (Eds.), Fast Software Encryption. XI, 485 pages. 2004.

Vol. 3016: C. Lengauer, D. Batory, C. Consel, M. Odersky (Eds.), Domain-Specific Program Generation. XII, 325 pages. 2004.

Table of Contents

Rob Tristan Gerth: 1956–2003 1

Static Program Analysis via 3-Valued Logic 15
Thomas W. Reps, Mooly Sagiv, and Reinhard Wilhelm

Deductive Verification of Pipelined Machines
Using First-Order Quantification 31
Sandip Ray and Warren A. Hunt, Jr.

A Formal Reduction for Lock-Free Parallel Algorithms 44
Hui Gao and Wim H. Hesselink

An Efficiently Checkable, Proof-Based Formulation of Vacuity
in Model Checking 57
Kedar S. Namjoshi

Termination of Linear Programs 70
Ashish Tiwari

Symbolic Model Checking of Non-regular Properties 83
Martin Lange

Proving More Properties with Bounded Model Checking 96
Mohammad Awedh and Fabio Somenzi

Parallel LTL-X Model Checking of High-Level Petri Nets
Based on Unfoldings 109
Claus Schröter and Victor Khomenko

Using Interface Refinement to Integrate Formal Verification
into the Design Cycle 122
Jacob Chang, Sergey Berezin, and David L. Dill

Indexed Predicate Discovery for Unbounded System Verification 135
Shuvendu K. Lahiri and Randal E. Bryant

Range Allocation for Separation Logic 148
Muralidhar Talupur, Nishant Sinha, Ofer Strichman, and Amir Pnueli

An Experimental Evaluation of Ground Decision Procedures 162
Leonardo de Moura and Harald Rueß

DPLL(T): Fast Decision Procedures 175
Harald Ganzinger, George Hagen, Robert Nieuwenhuis, Albert Oliveras, and Cesare Tinelli

Verifying ω-Regular Properties of Markov Chains 189
Doron Bustan, Sasha Rubin, and Moshe Y. Vardi

Statistical Model Checking of Black-Box Probabilistic Systems 202
Koushik Sen, Mahesh Viswanathan, and Gul Agha

Compositional Specification and Model Checking in GSTE 216
Jin Yang and Carl-Johan H. Seger

GSTE Is Partitioned Model Checking 229
Roberto Sebastiani, Eli Singerman, Stefano Tonetta, and Moshe Y. Vardi

Stuck-Free Conformance 242
Cédric Fournet, Tony Hoare, Sriram K. Rajamani, and Jakob Rehof

Symbolic Simulation, Model Checking and Abstraction with Partially Ordered Boolean Functional Vectors 255
Amit Goel and Randal E. Bryant

Functional Dependency for Verification Reduction 268
Jie-Hong R. Jiang and Robert K. Brayton

Verification via Structure Simulation 281
Niel Immerman, Alexander Rabinovich, Thomas W. Reps, Mooly Sagiv, and Great Yorsh

Symbolic Parametric Safety Analysis of Linear Hybrid Systems with BDD-Like Data-Structures 295
Farn Wang

Abstraction-Based Satisfiability Solving of Presburger Arithmetic 308
Daniel Kroening, Joël Ouaknine, Sanjit A. Seshia, and Ofer Strichman

Widening Arithmetic Automata 321
Constantinos Bartzis and Tevfik Bultan

Why Model Checking Can Improve WCET Analysis 334
Alexander Metzner

Regular Model Checking for LTL(MSO) 348
Parosh Aziz Abdulla, Bengt Jonsson, Marcus Nilsson, Julien d'Orso, and Mayank Saksena

Image Computation in Infinite State Model Checking 361
Alain Finkel and Jérôme Leroux

Abstract Regular Model Checking 372
Ahmed Bouajjani, Peter Habermehl, and Tomáš Vojnar

Global Model-Checking of Infinite-State Systems 387
Nir Piterman and Moshe Y. Vardi

QB or Not QB: An Efficient Execution Verification Tool for Memory Orderings 401
Ganesh Gopalakrishnan, Yue Yang, and Hemanthkumar Sivaraj

Verification of an Advanced MIPS-Type Out-of-Order Execution Algorithm 414
Tamarah Arons

Automatic Verification of Sequential Consistency for Unbounded Addresses and Data Values 427
Jesse Bingham, Anne Condon, Alan J. Hu, Shaz Qadeer, and Zhichuan Zhang

Efficient Modeling of Embedded Memories in Bounded Model Checking .. 440
Malay K. Ganai, Aarti Gupta, and Pranav Ashar

Understanding Counterexamples with `explain` 453
Alex Groce, Daniel Kroening, and Flavio Lerda

ZAPATO: Automatic Theorem Proving for Predicate Abstraction Refinement 457
Thomas Ball, Byron Cook, Shuvendu K. Lahiri, and Lintao Zhang

JNuke: Efficient Dynamic Analysis for Java 462
Cyrille Artho, Viktor Schuppan, Armin Biere, Pascal Eugster, Marcel Baur, and Boris Zweimüller

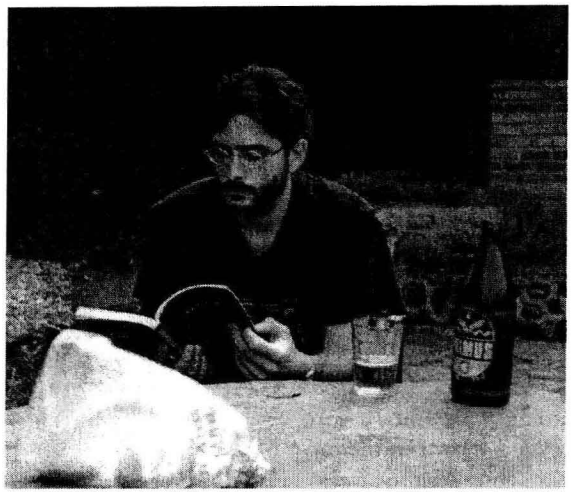
The HiVy Tool Set 466
Paula J. Pingree and Erich Mikk

OBSSLICE: A Timed Automata Slicer Based on Observers 470
Víctor Braberman, Diego Garbervetsky, and Alfredo Olivero

The UCLID Decision Procedure 475
Shuvendu K. Lahiri and Sanjit A. Seshia

MCK: Model Checking the Logic of Knowledge 479
Peter Gammie and Ron van der Meyden

Zing: A Model Checker for Concurrent Software 484
Tony Andrews, Shaz Qadeer, Sriram K. Rajamani, Jakob Rehof, and Yichen Xie



Kijereshi, Tanzania, 1994

HET KOMT WEL VOOR

"Gedaan in het gesloten seizoen der dromen"
Lucebert

het komt wel voor
dat de deur in het slot valt
de stilte plotseling intreedt
de angst toeslaat
men in een leegte staart –

het komt wel voor
dat een man van in de veertig
met ontstelde ogen toeziet
hoe de vingers zich in elkaar
wringen, voelen moet hoe de
adem stokt in de keel –

het komt wel voor
dat men dan de dood ontmoet

Wim Gerth
28 November 2003

Rob Tristan Gerth: 1956–2003

On Friday November 28, 2003, computer scientist and logician Rob Gerth died from sudden cardiac arrest. It is impossible to say all that the loss of Rob means to Intel, to the verification community, and to each of us personally.

As a corporation, Intel has lost a world-renowned authority on formal modeling and verification. Rob brought an independence of thought and agility of mind that are the hallmarks of a rare intellect. He was one of the few people with the knowledge and experience to meet the challenges we face in verifying micro-architectural protocols; we hope we can find a way to carry on his legacy.

As a community, we have lost not just a key technical contributor but part of our scientific conscience. It was in Rob's nature to ask "Why?", even when the answer seemed obvious. He brought a commitment to truth and high standards that was alternately challenging, frustrating, and inspiring; we will sorely miss it.

As family, friends and colleagues, we will remember and cherish Rob's warmth and love, his knowledge and openness in sharing it, his dry sense of humor, the way only he could read Toon Tellegen stories, and – perhaps most of all – his contagious laughter.

Rob's passion for knowledge reached far beyond computer science and logic: it embraced science, history, literature, art and music. The 2004 Proceedings of the 16th International Conference on Computer Aided Verification are dedicated to him. This article in the Proceedings surveys highlights of Rob's scientific career, followed by excerpts taken from some of the many tributes sent for Rob's funeral by friends and colleagues from around the world. The list of contributors, though too long to be printed here, is itself a tribute to Rob's impact on us all.

May 2004

John O'Leary & Marly Roncken
Intel

R. Alur and D.A. Peled (Eds.): CAV 2004, LNCS 3114, pp. 1–14, 2004.

Rob Gerth, Program Verifier par Excellence: His Research

Going through Rob Gerth's contributions to program semantics and verification, and tools for the latter, one is struck by his almost incredible versatility, total commitment, and scientific depth.

Starting in 1981 with a proof system for Brinch Hansen's monitor-based language Distributed Processes [1], he followed with an important paper on "Transition Logic: How to Reason about Temporal Properties in a Compositional Way" [2], coauthored papers on "Compositional Semantics for Real-Time Distributed Computing" for the predecessor of LICS [3], with its Full-Abstraction proof [4], a (sound and relatively complete) "Proof System for Concurrent Ada Programs" in *Science of Computer Programming* [5], and a far reaching paper in 1986 "Monitors Revisited: A First Step towards Verifying Object-Oriented Systems" [6], far before the general research public in computer science realized the importance of concepts like compositionality, formalized real-time semantics, or relatively complete proof systems for monitor-based and object-oriented languages.

This list continues to be extended in the same break-through baffling fashion: Coauthor of full-abstract semantics for Statecharts and concurrent Prolog [7, 8], "Rooting UNITY" [9], his Program Refinement and Self-Modifying Code [10, 11], coauthored papers for CONCUR [12, 13] or Reliable Distributed Systems [14]. Who else in those years cared for investigating fully abstract program semantics, verifying fault-tolerant distributed programs, self-modifying programs, interface refinement, and the now crucial concept of compositional refinement?

Having reached the limits of what can reasonably be verified *in principle* by hand, Rob saw that the time of automated verification had arrived and devoted himself with the same ruthless interest and intrepidity to developing foundations of abstract interpretation, model checking and automated refinement tools – to allow applications at industrial scale. The focus in his work now shifts to handling state explosion in (real-time) model checking.

To this end, he developed partial-order techniques [15, 16] and other advanced techniques like on-the-fly model checking [17] and abstraction [18] – the latter with his "very own" Ph.D. student Dennis Dams and with Orna Grumberg. The foundational aspects of abstract interpretation in model checking were first presented at a memorable PROCOMET workshop in San Miniato [19], and culminated in 1997 in a TOPLAS seminal paper [20] and application paper [21].

At the end of this period, Rob organised the ESPRIT project VIRES (Verifying Industrial Reactive Systems) where the developed theory and tools were applied to the verification of an industrial bus protocol. This project was his legacy to Europe, and the beginning of a new era in the verification of large systems. When Rob left the Technical University Eindhoven for Intel at the end of 1997, VIRES found a suitable new project lead in his former Ph.D student Dennis Dams.

Rob's "warming up" exercise at Intel was the ambitious exploratory project of formally verifying arithmetic hardware units to their IEEE specifications [22]. The technology and methodology developed in that project are used routinely

today to verify floating-point functionality in Intel's Microprocessor design projects.

He subsequently went back to a more familiar domain, developing a linear-time temporal logic – dubbed ForSpec [23]. The uniqueness of Forspec lies in its many special features for hardware specification, motivated by many Intel engineering years of both edge-cutting and practical design and validation. Rob's unique blend of theoretical knowledge and practical experience in formal semantics and model checking invariably prevented inconsistencies and efficiency hazards, and helped solve the most difficult roadblocks. ForSpec is widely used in Intel, and has been incorporated in OpenVera^{TM}, a language for hardware testbenches and assertions that is supported by a broad network of CAD companies.

Just weeks before his death, Rob presented the first results of what he called his "bit-vector compiler" – software he had been developing to relate protocol models over abstract data types to ditto models over "hardware" datatypes, i.e. bits and bit-vectors. Following up on [24], the compiler is part of Rob's protocol verification programme and perhaps the most cherished and ambitious project of his life. A life which he did not anticipate would end any time soon.

If Edsger Wiebe Dijkstra, another Dutchman, opened the eyes of computer scientists for the value of proving programs correct, then in Rob Tristan Gerth a worthy modern-day successor and polymath was incarnated, whose own unique vision furthered the feasibility of Dijkstra's programme. We shall all miss Rob's enthusiasm, ruthless intellectual curiosity, and relentless energy.

Selected List of Publications

1. M. Roncken, R. Gerth, and W. P. de Roever. A proof system for Brinch Hansen's distributed processes. In *Proceedings of the GI Jahrestagung*, pages 88–95, 1981.
2. R. Gerth. Transition logic: How to reason about temporal properties in a compositional way. In *16th ACM Symp. on Theory of Computing*, pages 39–50. ACM Press, 1984.
3. R. Koymans, R. K. Shyamasundar, W. P. de Roever, R. Gerth, and S. Arun-Kumar. Compositional semantics for real-time distributed computing. In R. Parikh, editor, *Logic of Programs*, volume 193 of *LNCS*, pages 167–189. Springer, 1985.
4. C. Huizing, R. Gerth, and W. P. deRoever. Full abstraction of a real-time denotational semantics for an OCCAM-like language. In *14th ACM Symp. on Principles of Programming Languages*, pages 223–236. ACM Press, 1987.
5. R. Gerth and W. P. de Roever. A proof system for concurrent Ada programs. *Science of Computer Programming*, 4(2):159–204, 1984.
6. R. Gerth and W. P. de Roever. Proving monitors revisited: a first step towards verifying object oriented systems. *Fundamenta Informatica*, 9(4):371–399, 1986.
7. C. Huizing, R. Gerth, and W. P. de Roever. Modeling statecharts behaviour in a fully abstract way. In M. Dauchet and M. Nivat, editors, *13th Colloq. on Trees in Algebra and Programming*, volume 299 of *LNCS*, pages 271–294. Springer, 1988.
8. R. Gerth, M. Codish, Y. Lichtenstein, and E. Y. Shapiro. Fully abstract denotational semantics for flat concurrent Prolog. In *3rd Symp. on Logic in Computer Science*, pages 320–335. IEEE Computer Society, 1988.

9. R. Gerth and A. Pnueli. Rooting UNITY. *ACM SIGSOFT Software Engineering Notes*, 14(3):11–19, 1989.
10. R. Gerth. Foundations of compositional program refinement - safety properties. In J. W. de Bakker, W. P. de Roever, and G. Rozenberg, editors, *Stepwise Refinement of Distributed Systems: Models, Formalisms, Correctness*, volume 430 of *LNCS*, pages 777–807. Springer, 1989.
11. R. Gerth. Formal verification of self modifying code. In *Int. Conf. for Young Computer Scientists*, pages 305–313. International Acad. Publishers, China, 1991.
12. R. Gerth, R. Kuiper, and J. Segers. Interface refinement in reactive systems. In R. Cleaveland, editor, *3rd Int. Conf.on Concurrency Theory*, volume 630 of *LNCS*, pages 77–93. Springer, 1992.
13. S. Zhou, R. Gerth, and R. Kuiper. Transformations preserving properties and properties preserved by transformations in fair transition systems. In E. Best, editor, *4th Int. Conf. on Concurrency Theory*, volume 715 of *LNCS*, pages 353–367. Springer, 1993.
14. H. Schepers and R. Gerth. A compositional proof theory for fault tolerant real-time distributed systems. In *12th Symp. on Reliable Distributed Systems*, pages 34–43. IEEE Computer Society, 1993.
15. D. Dams, R. Gerth, B. Knaack, and R. Kuiper. Partial-order reduction techniques for real-time model checking. *Formal Aspects of Computing*, 10(5-6):132–152, 1998.
16. R. Gerth, R. Kuiper, D. Peled, and W. Penczek. A partial order approach to branching time logic model checking. *Inf. and Comp.*, 150(2):132–152, 1999.
17. R. Gerth, D. Peled, M. Y. Vardi, and P. Wolper. Simple on-the-fly automatic verification of linear temporal logic. In *15th IFIP WG6.1 Int. Symp. on Protocol Specification, Testing and Verification*, volume 38 of *IFIP Conference Proceedings*, pages 3–18. Chapman & Hall, 1995.
18. D. Dams, O. Grumberg, and R. Gerth. Generation of reduced models for checking fragments of CTL. In *CAV*, LNCS, pages 479–490. Springer, 1993.
19. D. Dams, O. Grumberg, and R. Gerth. Abstract interpretation of reactive systems: Abstractions preserving $\forall$CTL*, $\exists$CTL* and CTL*. In E.-R. Olderog, editor, *IFIP WG2.1/WG2.2/WG2.3 Working Conf. on Programming Concepts, Methods and Calculi*, IFIP Transactions. North-Holland/Elsevier, June 1994.
20. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. on Programming Languages and Systems*, 19(2):253–291, 1997.
21. D. Dams and R. Gerth. The bounded retransmission protocol revisited. In F. Moller, editor, *2nd Int. Workshop on Verification of Infinite State Systems*, volume 9 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 1997.
22. J. O'Leary, X. Zhao, C.-J. H. Seger, and R. Gerth. Formally verifying IEEE compliance of floating-point hardware. *Intel Technical Journal*, First Quarter 1999.
23. R. Armoni, L. Fix, A. Flaisher, R. Gerth, B. Ginsburg, T. Kanza, A. Landver, S. Mador-Haim, E. Singerman, A. Tiemeyer, M. Y. Vardi, and Y. Zbar. A new temporal property-specification language. In J.-P. Katoen and P. Stevens, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 2280 of *LNCS*, pages 296–311. Springer, 2002.
24. R. Gerth. Sequential consistency and the lazy caching algorithm. *Distributed Computing*, 12(2-3):57–59, 1999.