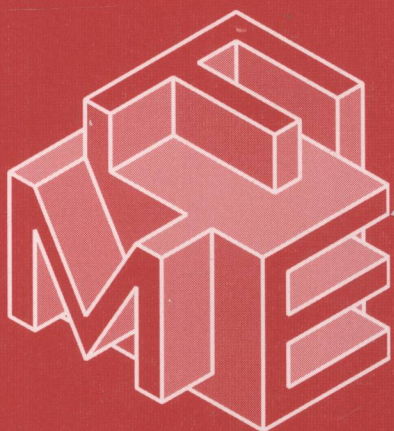


LNCS 4085

Jayadev Misra
Tobias Nipkow
Emil Sekerinski (Eds.)

FM 2006: Formal Methods

14th International Symposium on Formal Methods
Hamilton, Canada, August 2006
Proceedings



Springer

TP311.52-53

F723.3

2006

Jayadev Misra Tobias Nipkow
Emil Sekerinski (Eds.)

FM 2006: Formal Methods

14th International Symposium on Formal Methods
Hamilton, Canada, August 21-27, 2006
Proceedings



Springer



E200603977

Volume Editors

Jayadev Misra

University of Texas at Austin

Department of Computer Sciences, Taylor Hall

1 University Station, C0500, Austin, Texas 78712-1188, USA

E-mail: misra@cs.utexas.edu

Tobias Nipkow

Technische Universität München

Institut für Informatik

Boltzmannstr. 3, 85748 Garching, Germany

E-mail: nipkow@in.tum.de

Emil Sekerinski

McMaster University

Department of Computing and Software

1280 Main Street West, Hamilton, Ontario, L8S 4K1 Canada

E-mail: emil@mcmaster.ca

Library of Congress Control Number: 2006930417

CR Subject Classification (1998): D.2, F.3, D.3, D.1, J.1, K.6, F.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-540-37215-6 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-37215-8 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11813040 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of Formal Methods 2006, the 14th International Symposium on Formal Methods, held at McMaster University, Hamilton, Canada, during August 21-27, 2006. Formal Methods Europe (FME, www.fmeurope.org) is an independent association which aims to stimulate the use of, and research on, formal methods for system development. The first symposium in this series was VDM Europe in 1987. The scope of the symposium has grown since then, encompassing all aspects of software and hardware which are amenable to formal analysis. As in the previous years, this symposium brings together researchers, tool developers, vendors and users.

We received 145 submissions from 31 countries, making it a truly international event. Each submission was carefully refereed by at least three reviewers. The Program Committee selected 36 papers for presentation at the symposium, after an intensive, in-depth discussion. We would like to thank all the Program Committee members and the referees for their excellent and efficient work.

Apart from the regular contributions, there were five invited talks for the general symposium (Ernie Cohen, Nicholas Griffin, Thomas A. Henzinger, Peter Lindsay and George Necula); the contribution of Henzinger (with Sifakis as a co-author) and an abstract from Cohen are included in this volume.

Nicholas Griffin gave a general and informal talk about Russell's work in logic and the foundations of mathematics in the early years of the twentieth century. It focussed on the philosophical views that underlay Russell's attempts to solve the Russell paradox (and several others) which culminated in the ramified theory of types.

The FM 2006 symposium was planned to include four workshops and ten tutorials. Additionally, there was a Doctoral Symposium which included presentations by doctoral students, and a Poster and Tool Exhibition.

An Industry Day was organized by the Formal Techniques Industrial Association (ForTIA) alongside the main symposium. This was directly related to the main theme of the symposium: the use of well-founded formal methods in the industrial practice of software design, development and maintenance. The theme of the Industry Day in this symposium was "Formal Methods for Security and Trust in Industrial Applications." There were eight invited talks for Industry Day (Randolph Johnson, Jan Jürjens, Scott A. Lintelman, Dusko Pavlovic, Werner Stephan, Michael Waidner, Jim Woodcock and David von Oheimb); abbreviated versions of some of the talks are included in this volume.

The electronic submission, refereeing and Program Committee discussions would not have been possible without support of the EasyChair system, developed by Andrei Voronkov at the University of Manchester, UK. In addition to developing a system of great flexibility, Andrei was available for help and advice throughout; our heart-felt thanks to him. Our thanks to Springer, and,

particularly, Ursula Barth, Anna Kramer and Frank Holzwarth, for help with preparation of this volume.

August 2006

Jayadev Misra
Tobias Nipkow
Emil Sekerinski

Symposium Organization

We are grateful to the Computing and Software Center at McMaster University, Hamilton, Canada and Formal Methods Europe for organizing FM 2006. Our special thanks to the faculty, students and staff of McMaster University who volunteered their time in the Organizing Committee.

Symposium Chairs

General Chair	Emil Sekerinski, McMaster University, Canada
Program Chairs	Jayadev Misra, University of Texas, Austin, USA
	Tobias Nipkow, Universität München, Germany
Industry Day Chairs	Volkmar Lotz, SAP Research Labs, France
	Asuman Suenbuel, SAP Research Labs, USA
Tools and Poster Chair	Marsha Chechik, University of Toronto, Canada
Workshops Chair	Tom Maibaum, McMaster University, Canada
Tutorials Chair	Jin Song Dong, National University, Singapore
Doctoral Symposium Chair	Ana Cavalcanti, University of York, UK
	Augusto Sampaio, UFPE, Brazil
	Jim Woodcock, University of York, UK
Sponsorship Chair	Jürgen Dingel, Queen's University, Canada

Organizing Committee at McMaster University

Publicity	Wolfram Kahl, Alan Wass yng, Jeff Zucker
Book Exhibition	Spencer Smith
Tools and Posters	Spencer Smith
Social Events	Ridha Khedri
Facilities Co-ordination	William Farmer, Mark Lawford
Events Co-ordination	Ryszard Janicki
Finances	Ryszard Janicki
Website Services	Doris Burns, Jan Maibaum

Program Committee

Jean-Raymond Abrial, ETH, Zurich, Switzerland
Alex Aiken, Stanford University, Stanford, USA
Keijiro Araki, Kyushu University, Fukuoka, Japan
Ralph-Johan Back, Abo Akademi, Turku, Finland

Gilles Barthe, INRIA at Sophia-Antipolis, France
 David Basin, ETH, Zurich, Switzerland
 Frank de Boer, CWI, Amsterdam, The Netherlands
 Ed Brinksma, Embedded Systems Institute, Eindhoven, The Netherlands
 Michael Butler, University of Southampton, Southampton, UK
 Rance Cleaveland, University of Maryland, College Park, USA
 Jorge Cuellar, Siemens Research, Munich, Germany
 Werner Damm, OFFIS, Oldenburg, Germany
 Javier Esparza, University of Stuttgart, Stuttgart, Germany
 José Fiadeiro, University of Leicester, UK
 Susanne Graf, Verimag, Grenoble, France
 Ian Hayes, University of Queensland, Queensland, Australia
 Gerard Holzmann, NASA/JPL Labs, Pasadena, USA
 Cliff Jones, University of Newcastle upon Tyne, UK
 Axel van Lamsweerde, Université Catholique de Louvain, Belgium
 Gary T. Leavens, Iowa State University, Ames, USA
 Rustan Leino, Microsoft Research, Redmond, USA
 Xavier Leroy, INRIA, Rocquencourt, France
 Dominique Méry, LORIA and Université Henri Poincaré, Nancy, France
 Carroll Morgan, University of New South Wales, NSW, Australia
 David Naumann, Stevens Institute of Technology, Hoboken, USA
 Ernst-Rüdiger Olderog, University of Oldenburg, Oldenburg, Germany
 Paritosh Pandya, TIFR, Mumbai, India
 Sriram Rajamani, Microsoft Research, Bangalore, India
 John Rushby, SRI International, Menlo Park, USA
 Steve Schneider, University of Surrey, Guildford, UK
 Vitaly Shmatikov, University of Texas, Austin, USA
 Bernhard Steffen, University of Dortmund, Dortmund, Germany
 P.S. Thiagarajan, National University of Singapore, Singapore
 Martin Wirsing, Universität München, Germany
 Pierre Wolper, Université de Liège, Liège, Belgium

External Reviewers

J. Abendroth	Andrew Appel	Krzysztof Apt
Yuji Arichika	Eugene Asarin	Anindya Banerjee
Mike Barnett	Don Batory	Maurice ter Beek
Yves Bertot	Sylvie Boldo	Marcello Bonsangue
Laura Brandan Briones	Achim Brucker	Dominique Cansell
David Carrington	Paul Caspi	Antonio Cau
Patrice Chalin	Tom Chothia	Dave Clarke
Joey Coleman	Robert Colvin	Olivier Constant
Phil Cook	William Cook	Karl Crary
Maximiliano Cristia	Adrian Curic	Roberto Delicata

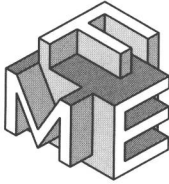
Henning Dierks
 Guillaume Dufay
 E. Allen Emerson
 Bernd Fischer
 Marcelo Frias
 Madhu Gopinathan
 Stefan Hallerstede
 Tobias Heindel
 Wim Hesselink
 Hardi Hungenar
 Johan Jeuring
 Aditya Kanade
 Joseph Kiniry
 Piotr Kordy
 Tomas Krilavicius
 Ruurd Kuiper
 Linas Laibinis
 David Lesens
 Michael Luttenberger
 Erik Arne Mathiesen
 Farhad Mehta
 Ali Mili
 Anders Moller
 Prasad Naldurg
 Dirk Nowotka
 Anne Pacalet
 Mariela Pavlova
 David Pichardie
 Mike Poppleton
 Alexander Pretschner
 Hridesh Rajan
 Abdolbaghi Rezazadeh
 Abhik Roychoudhury
 David Rydeheard
 Norbert Schirmer
 Paul Sevinc
 Colin Snook
 Marielle Stoelinga
 Douglas Stuart
 Helen Treharne
 Laurent Voisin
 Thai Son Wang
 Bernd Westphal
 Jim Woodcock
 Letu Yang

Juegen Doser
 Andy Edmunds
 Neil Evans
 John Fitzgerald
 Paul Gibson
 Bhargav Gulavani
 Klaus Havelund
 Rolf Hennicker
 Matthias Hölzl
 Daniel Jackson
 Warren A. Hunt Jr.
 Stephanie Kemper
 Alexander Knapp
 Piotr Kosiuczenko
 Ingolf Krueger
 Marcel Kyas
 Rom Langerak
 Kamal Lodaya
 Monika Maidl
 Tim McComb
 Roland Meyer
 Antoine Mine
 Michael Möller
 Rocco De Nicola
 Peter O'Hearn
 Joachim Parrow
 Thomas Peikenkamp
 Ken Pierce
 Sanjiva Prasad
 Cyril Proch
 H. Rajasekaran
 M. Birna van Riemsdijk
 Oliver Ruething
 Mannu Satpathy
 Gerardo Schneider
 Murali Sitaraman
 Martin Steffen
 Ketil Stølen
 Martyn Thomas
 Stavros Tripakis
 Marina de Vos
 Andrzej Wasowski
 Luke Wildman
 Fei Xie
 Pamela Zave

Paul Hanks Drielsma
 Martin Ellis
 Dirk Fahland
 Martin Fränzle
 Simon Goldsmith
 Christian Haack
 James Heather
 Martin Henson
 Marieke Huisman
 Suresh Jagannathan
 Sven Jörges
 Stefan Kiefer
 Barbara König
 Pavel Krcal
 Wouter Kuijper
 Ralf Laemmel
 Kim Larsen
 Antònia Lopes
 Joao Marques-Silva
 Alistair McEwan
 Ronald Middelkoop
 Bill Mitchell
 Peter Müller
 Aditya Nori
 David von Oheimb
 Dirk Pattinson
 Simon Peyton-Jones
 Jaco van de Pol
 Viorel Preoteasa
 Harald Raffelt
 Axel Rauschmayer
 Robby
 Theo Ruys
 Andreas Schäfer
 Stefan Schwoon
 Graeme Smith
 Mark-Oliver Stehr
 Harald Störrle
 Christian Topnik
 Emilio Tuosto
 Thomas Wahl
 Heike Wehrheim
 Martin Wildmoser
 Alex Yakovlev
 Gefei Zhang

Sponsors

We are thankful for the organizational support from FME and Formal Techniques Industrial Association (ForTIA). We gratefully acknowledge sponsorships from the following organizations: Microsoft Research, Tourism Hamilton, SAP Labs France, Software Quality Research Laboratory of McMaster University, and Faculty of Engineering of McMaster University.



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

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

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Lecture Notes in Computer Science

For information about Vols. 1–4017

please contact your bookseller or Springer

- Vol. 4144: T. Ball, R.B. Jones (Eds.), *Computer Aided Verification*. XV, 564 pages. 2006.
- Vol. 4127: E. Damiani, P. Liu (Eds.), *Data and Applications Security XX*. X, 319 pages. 2006.
- Vol. 4121: A. Biere, C.P. Gomes (Eds.), *Theory and Applications of Satisfiability Testing - SAT 2006*. XII, 438 pages. 2006.
- Vol. 4115: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Computational Intelligence and Bioinformatics, Part III*. XXI, 803 pages. 2006. (Sublibrary LNBI).
- Vol. 4114: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Computational Intelligence, Part II*. XXVII, 1337 pages. 2006. (Sublibrary LNAI).
- Vol. 4113: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Intelligent Computing, Part I*. XXVII, 1331 pages. 2006.
- Vol. 4112: D.Z. Chen, D. T. Lee (Eds.), *Computing and Combinatorics*. XIV, 528 pages. 2006.
- Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *Formal Methods for Components and Objects*. VIII, 447 pages. 2006.
- Vol. 4109: D.-Y. Yeung, J.T. Kwok, A. Fred, F. Roli, D. de Ridder (Eds.), *Structural, Syntactic, and Statistical Pattern Recognition*. XXI, 939 pages. 2006.
- Vol. 4108: J.M. Borwein, W.M. Farmer (Eds.), *Mathematical Knowledge Management*. VIII, 295 pages. 2006. (Sublibrary LNAI).
- Vol. 4106: T.R. Roth-Berghofer, M.H. Göker, H. A. Güvenir (Eds.), *Advances in Case-Based Reasoning*. XIV, 566 pages. 2006. (Sublibrary LNAI).
- Vol. 4104: T. Kunz, S.S. Ravi (Eds.), *Ad-Hoc, Mobile, and Wireless Networks*. XII, 474 pages. 2006.
- Vol. 4099: Q. Yang, G. Webb (Eds.), *PRICAI 2006: Trends in Artificial Intelligence*. XXVIII, 1263 pages. 2006. (Sublibrary LNAI).
- Vol. 4098: F. Pfenning (Ed.), *Term Rewriting and Applications*. XIII, 415 pages. 2006.
- Vol. 4097: X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D.C. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing*. XXVII, 1034 pages. 2006.
- Vol. 4096: E. Sha, S.-K. Han, C.-Z. Xu, M.H. Kim, L.T. Yang, B. Xiao (Eds.), *Embedded and Ubiquitous Computing*. XXIV, 1170 pages. 2006.
- Vol. 4094: O. H. Ibarra, H.-C. Yen (Eds.), *Implementation and Application of Automata*. XIII, 291 pages. 2006.
- Vol. 4093: X. Li, O.R. Zaiane, Z. Li (Eds.), *Advanced Data Mining and Applications*. XXI, 1110 pages. 2006. (Sublibrary LNAI).
- Vol. 4092: J. Lang, F. Lin, J. Wang (Eds.), *Knowledge Science, Engineering and Management*. XV, 664 pages. 2006. (Sublibrary LNAI).
- Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), *Journal on Data Semantics VI*. XI, 211 pages. 2006.
- Vol. 4088: Z.-Z. Shi, R. Sadananda (Eds.), *Agent Computing and Multi-Agent Systems*. XVII, 827 pages. 2006. (Sublibrary LNAI).
- Vol. 4085: J. Misra, T. Nipkow, E. Sekerinski (Eds.), *FM 2006: Formal Methods*. XV, 620 pages. 2006.
- Vol. 4079: S. Etalle, M. Truszczyński (Eds.), *Logic Programming*. XIV, 474 pages. 2006.
- Vol. 4077: M.-S. Kim, K. Shimada (Eds.), *Advances in Geometric Modeling and Processing*. XVI, 696 pages. 2006.
- Vol. 4076: F. Hess, S. Pauli, M. Pohst (Eds.), *Algorithmic Number Theory*. X, 599 pages. 2006.
- Vol. 4075: U. Leser, F. Naumann, B. Eckman (Eds.), *Data Integration in the Life Sciences*. XI, 298 pages. 2006. (Sublibrary LNBI).
- Vol. 4074: M. Burmester, A. Yasinac (Eds.), *Secure Mobile Ad-hoc Networks and Sensors*. X, 193 pages. 2006.
- Vol. 4073: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), *Smart Graphics*. XI, 263 pages. 2006.
- Vol. 4072: M. Harders, G. Székely (Eds.), *Biomedical Simulation*. XI, 216 pages. 2006.
- Vol. 4071: H. Sundaram, M. Naphade, J.R. Smith, Y. Rui (Eds.), *Image and Video Retrieval*. XII, 547 pages. 2006.
- Vol. 4070: C. Priami, X. Hu, Y. Pan, T.Y. Lin (Eds.), *Transactions on Computational Systems Biology V*. IX, 129 pages. 2006. (Sublibrary LNBI).
- Vol. 4069: F.J. Perales, R.B. Fisher (Eds.), *Articulated Motion and Deformable Objects*. XV, 526 pages. 2006.
- Vol. 4068: H. Schärfe, P. Hitzler, P. Øhrstrøm (Eds.), *Conceptual Structures: Inspiration and Application*. XI, 455 pages. 2006. (Sublibrary LNAI).
- Vol. 4067: D. Thomas (Ed.), *ECOOP 2006 – Object-Oriented Programming*. XIV, 527 pages. 2006.
- Vol. 4066: A. Rensink, J. Warmer (Eds.), *Model Driven Architecture – Foundations and Applications*. XII, 392 pages. 2006.
- Vol. 4065: P. Perner (Ed.), *Advances in Data Mining*. XI, 592 pages. 2006. (Sublibrary LNAI).
- Vol. 4064: R. Büschkes, P. Laskov (Eds.), *Detection of Intrusions and Malware & Vulnerability Assessment*. X, 195 pages. 2006.

- Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.
- Vol. 4062: G. Wang, J.F. Peters, A. Skowron, Y. Yao (Eds.), Rough Sets and Knowledge Technology. XX, 810 pages. 2006. (Sublibrary LNAI).
- Vol. 4061: K. Miesenberger, J. Klaus, W. Zagler, A. Karshmer (Eds.), Computers Helping People with Special Needs. XXIX, 1356 pages. 2006.
- Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning, and Computation. XXXVIII, 643 pages. 2006.
- Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.
- Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.
- Vol. 4057: J.P.W. Pluim, B. Likas, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.
- Vol. 4056: P. Flocchini, L. Gasieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.
- Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.
- Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.
- Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.
- Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XXIV, 603 pages. 2006.
- Vol. 4051: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part I. XXIII, 729 pages. 2006.
- Vol. 4049: S. Parsons, N. Maudet, P. Moraitis, I. Rahwan (Eds.), Argumentation in Multi-Agent Systems. XIV, 313 pages. 2006. (Sublibrary LNAI).
- Vol. 4048: L. Goble, J.-J.C. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).
- Vol. 4047: M. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.
- Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.
- Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).
- Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.
- Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.
- Vol. 4042: D. Bell, J. Hong (Eds.), Flexible and Efficient Information Handling. XVI, 296 pages. 2006.
- Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.
- Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.
- Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.
- Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.
- Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.
- Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), Developments in Language Theory. XII, 456 pages. 2006.
- Vol. 4035: T. Nishita, Q. Peng, H.-P. Seidel (Eds.), Advances in Computer Graphics. XX, 771 pages. 2006.
- Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.
- Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performance Has its Price. X, 103 pages. 2006.
- Vol. 4032: O. Etzion, T. Kuflik, A. Motro (Eds.), Next Generation Information Technologies and Systems. XIII, 365 pages. 2006.
- Vol. 4031: M. Ali, R. Dapoigny (Eds.), Advances in Applied Artificial Intelligence. XXIII, 1353 pages. 2006. (Sublibrary LNAI).
- Vol. 4029: L. Rutkowski, R. Tadeusiewicz, L.A. Zadeh, J.M. Zurada (Eds.), Artificial Intelligence and Soft Computing – ICAISC 2006. XXI, 1235 pages. 2006. (Sublibrary LNAI).
- Vol. 4028: J. Kohlas, B. Meyer, A. Schiper (Eds.), Dependable Systems: Software, Computing, Networks. XII, 295 pages. 2006.
- Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreassen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).
- Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.
- Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.
- Vol. 4024: S. Donatelli, P.S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.
- Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).
- Vol. 4020: A. Bredendfeld, A. Jacoff, I. Noda, Y. Takahashi (Eds.), RoboCup 2005: Robot Soccer World Cup IX. XVII, 727 pages. 2006. (Sublibrary LNAI).
- Vol. 4019: M. Johnson, V. Vene (Eds.), Algebraic Methodology and Software Technology. XI, 389 pages. 2006.
- Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XVI, 474 pages. 2006.

¥615.00元

Table of Contents

Invited Talk

The Embedded Systems Design Challenge	1
<i>Thomas A. Henzinger, Joseph Sifakis</i>	

Interactive Verification

The Mondex Challenge: Machine Checked Proofs for an Electronic Purse	16
<i>Gerhard Schellhorn, Holger Grandy, Dominik Haneberg, Wolfgang Reif</i>	
Interactive Verification of Medical Guidelines	32
<i>Jonathan Schmitt, Alwin Hoffmann, Michael Balser, Wolfgang Reif, Mar Marcos</i>	
Certifying Airport Security Regulations Using the Focal Environment	48
<i>David Delahaye, Jean-Frédéric Étienne, Véronique Viguié Donzeau-Gouge</i>	
Proving Safety Properties of an Aircraft Landing Protocol Using I/O Automata and the PVS Theorem Prover: A Case Study	64
<i>Shinya Umeno, Nancy Lynch</i>	

Invited Talk

Validating the Microsoft Hypervisor	81
<i>Ernie Cohen</i>	

Formal Modelling of Systems

Interface Input/Output Automata	82
<i>Kim G. Larsen, Ulrik Nyman, Andrzej Wąsowski</i>	
Properties of Behavioural Model Merging	98
<i>Greg Brunet, Marsha Chechik, Sebastian Uchitel</i>	
Automatic Translation from <i>Circus</i> to Java	115
<i>Angela Freitas, Ana Lucia Caneca Cavalcanti</i>	
Quantitative Refinement <i>and</i> Model Checking for the Analysis of Probabilistic Systems	131
<i>Annabelle K. McIver</i>	

Real Time

Modeling and Validating Distributed Embedded Real-Time Systems with VDM++	147
<i>Marcel Verhoef, Peter Gorm Larsen, Jozef Hooman</i>	

Towards Modularized Verification of Distributed Time-Triggered Systems	163
<i>Jewgenij Botaschanjan, Alexander Gruler, Alexander Harhurin, Leonid Kof, Maria Spichkova, David Trachtenherz</i>	

Industrial Experience

A Story About Formal Methods Adoption by a Railway Signaling Manufacturer	179
<i>Stefano Bacherini, Alessandro Fantechi, Matteo Tempestini, Niccolò Zingoni</i>	

Partially Introducing Formal Methods into Object-Oriented Development: Case Studies Using a Metrics-Driven Approach	190
<i>Yujun Zheng, Jinquan Wang, Kan Wang, Jinyun Xue</i>	

Specification and Refinement

Compositional Class Refinement in Object-Z	205
<i>Tim McComb, Graeme Smith</i>	

A Proposal for Records in Event-B	221
<i>Neil Evans, Michael Butler</i>	

Pointfree Factorization of Operation Refinement	236
<i>José Nuno Oliveira, César Jesus Rodrigues</i>	

A Formal Template Language Enabling Metaproof	252
<i>Nuno Amálio, Susan Stepney, Fiona Polack</i>	

Programming Languages

Dynamic Frames: Support for Framing, Dependencies and Sharing Without Restrictions (Best Paper)	268
<i>Ioannis T. Kassios</i>	

Type-Safe Two-Level Data Transformation	284
<i>Alcino Cunha, José Nuno Oliveira, Joost Visser</i>	

Algebra

Feature Algebra	300
<i>Peter Höfner, Ridha Khedri, Bernhard Möller</i>	

Education

Using Domain-Independent Problems for Introducing Formal Methods	316
<i>Raymond Boute</i>	

Formal Modelling of Systems

Compositional Binding in Network Domains	332
<i>Pamela Zave</i>	
Formal Modeling of Communication Protocols by Graph Transformation	348
<i>Zarrin Langari, Richard Trefler</i>	
Feature Specification and Static Analysis for Interaction Resolution	364
<i>Marc Aiguier, Karim Berkani, Pascale Le Gall</i>	
A Fully General Operational Semantics for UML 2.0 Sequence Diagrams with Potential and Mandatory Choice	380
<i>Mass Soldal Lund, Ketil Stølen</i>	

Formal Aspects of Java

Towards Automatic Exception Safety Verification	396
<i>Xin Li, H. James Hoover, Piotr Rudnicki</i>	
Enforcer – Efficient Failure Injection	412
<i>Cyrille Valentin Artho, Armin Biere, Shinichi Honiden</i>	
Automated Boundary Test Generation from JML Specifications	428
<i>Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard</i>	
Formal Reasoning About Non-atomic JAVA CARD Methods in Dynamic Logic	444
<i>Wojciech Mostowski</i>	

Programming Languages

Formal Verification of a C Compiler Front-End	460
<i>Sandrine Blazy, Zaynah Dargaye, Xavier Leroy</i>	

A Memory Model Sensitive Checker for C# 476
Thuan Quang Huynh, Abhik Roychoudhury

Changing Programs Correctly: Refactoring with Specifications 492
Fabian Bannwart, Peter Müller

Mechanical Verification of Recursive Procedures Manipulating Pointers
Using Separation Logic 508
Viorel Preoteasa

Model Checking

Model-Based Variable and Transition Orderings for Efficient Symbolic
Model Checking 524
*Wendy Johnston, Kirsten Winter, Lionel van den Berg,
Paul Strooper, Peter Robinson*

Exact and Approximate Strategies for Symmetry Reduction in Model
Checking 541
Alastair F. Donaldson, Alice Miller

Monitoring Distributed Controllers: When an Efficient LTL Algorithm
on Sequences Is Needed to Model-Check Traces 557
Alexandre Genon, Thierry Massart, Cédric Meuter

PSL Model Checking and Run-Time Verification Via Testers 573
Amir Pnueli, Aleksandr Zaks

Industry Day: Abstracts of Invited Talks

Formal Methods for Security: Lightweight Plug-In or New Engineering
Discipline 587
Werner Stephan

Formal Methods in the Security Business: Exotic Flowers Thriving
in an Expanding Niche 592
David von Oheimb

Connector-Based Software Development: Deriving Secure Protocols 598
Dusko Pavlovic

Model-Based Security Engineering for Real 600
Jan Jürjens

Cost Effective Software Engineering for Security 607
D. Randolph Johnson

Formal Methods and Cryptography 612
Michael Backes, Birgit Pfitzmann, Michael Waidner

Verified Software Grand Challenge	617
<i>Jim Woodcock</i>	
Author Index	619