

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

Cliff B. Jones Zhiming Liu
Jim Woodcock (Eds.)

Formal Methods and Hybrid Real-Time Systems

Essays in Honour of Dines Bjørner and Zhou Chaochen
on the Occasion of Their 70th Birthdays

Volume Editors

Cliff B. Jones

Newcastle University, School of Computing Science

Newcastle upon Tyne, NE1 7RU, UK

E-mail: cliff.jones@ncl.ac.uk

Zhiming Liu

United Nations University, International Institute for Software Technology

Macao, China

E-mail: z.liu@iist.unu.edu

Jim Woodcock

University of York, Department of Computer Science

Heslington, York YO10 5DD, UK

E-mail: jim@cs.york.ac.uk

The illustration appearing on the cover of this book is the work of Daniel Rozenberg (DADARA).

Library of Congress Control Number: 2007935177

CR Subject Classification (1998): D.2, D.3, C.3, F.3-4, C.2, H.4

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743

ISBN-10 3-540-75220-X Springer Berlin Heidelberg New York

ISBN-13 978-3-540-75220-2 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 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12164615 06/3180 5 4 3 2 1 0



Dines Bjørner



Zhou Chaochen

Foreword

Two outstanding computer scientists will soon reach their 70th birthdays: Dines Bjørner was born on October 4, 1937 in Denmark and Zhou Chaochen was born on November 1, in the same year in China. To celebrate their birthdays, we present three LNCS volumes in their honour.

- *Formal Methods and Hybrid Real-Time Systems. Essays in Honour of Dines Bjørner and Zhou Chaochen on the Occasion of Their 70th Birthdays.* Papers presented at a Symposium held in Macao, China, September 24–25, 2007. LNCS volume 4700. Springer 2007.
- *Domain Modelling and the Duration Calculus.* International Training School, Shanghai, China, September 10–21, 2007. Advanced Lectures. LNCS volume 4710. Springer 2007.
- *Theoretical Aspects of Computing - ICTAC 2007.* 4th International Colloquium, Macao, China, September 26–28, 2007, Proceedings. LNCS volume 4711. Springer 2007.

DINES BJØRNER is known for his many contributions to the theory and practice of formal methods for software engineering. He is particularly associated with two formal methods, although his influence is far wider. He worked with Cliff Jones and others on the *Vienna Development Method (VDM)*, initially at IBM in Vienna. Later, he was involved in producing the *Rigorous Approach to Industrial Software Engineering (RAISE)* formal method with tool support. His three-volume *magnum opus* on software engineering covers *Abstraction and Modelling*, *Specification of Systems and Languages*, and *Domains, Requirements, and Software Design*. He was a professor at the Technical University of Denmark (DTU) in Lyngby, near Copenhagen. He was the founding director of the United Nations University International Institute for Software Technology (UNU-IIST) in Macao during the 1990s. He was a co-founder of VDM-Europe, which transformed to become Formal Methods Europe, an organisation that promotes the use of formal methods. Its 18 monthly symposia have become the leading academic events in formal methods. Dines Bjørner is a Knight of the Order of the Dannebrog and was awarded the John von Neumann Medal in Budapest in 1994. He received a Doctorate (*honoris causa*) from the Masaryk University in Brno in 2004. He is a Fellow of both the IEEE and the ACM.

ZHOU CHAOCHEN is known for his seminal contributions to the theory and practice of timed and hybrid systems. His distinguished academic career started as an undergraduate in mathematics and mechanics at Peking University (1954–58) and as a postgraduate at the Institute for Computing Technology in the Chinese Academy of Sciences (1963–67). He continued his career at Peking University and the Chinese Academy, until he made an extended visit to Oxford University

Computing Laboratory (1989–92) at the invitation of Sir Tony Hoare FRS. Here he was the prime instigator of *Duration Calculus*, an interval logic for real-time systems, developed as part of a European ESPRIT project on Provably Correct Systems. He made further extended visits during the periods 1990–92 and 1995–96, as a visiting professor at the Technical University of Denmark, Lyngby, at the invitation of Dines Bjørner. He was a Principal Research Fellow at UNU-IIST during the period 1992–97, before becoming its director, an appointment he held from 1997 to 2002. He is a member of the Chinese Academy of Sciences and the Third World Academy of Sciences.

We thank both Dines Bjørner and Zhou Chaochen for their years of generous, wise advice, to us and to their many other colleagues, students, and friends. They have both been unfailingly inspiring, enthusiastic, and encouraging.

July 2007

J.C.P.W.

Tabula Gratulatoria

Nazareno Aguirre	Anne Haxthausen	Ernst-Rüdiger Olderog
Bogdan Aman	Ian Hayes	Romain Péchoux
Damian Barsotti	He Jifeng	Miguel Palomino
Marc Bezem	Michael A. Jackson	Jun Pang
Nikolaj Bjørner	Tomasz Janowski	Jan Peleska
Javier Blanco	Cliff Jones	Martin Pěnička
Guillaume Bonfante	Mathai Joseph	André Platzer
Pontus Boström	Takashi Kitamura	Rosario Pugliese
Aske Wiid Brekling	John Knudsen	Brian Randell
Jan Bretschneider	Maciej Koutny	Silvio Ranise
Alan Burns	Padmanabhan Krishnan	Anders Ravn
Andrew Butterfield	Hans Langmaack	Wolfgang Reisig
Zining Cao	Ruggero Lanotte	Stefan Rieger
Pablo Castro	Alessandro Lapadula	Matteo Rossi
Haiyan Chen	Peter Gorm Larsen	Cesar Sanchez
Huowang Chen	Martin Leucker	J.W. Sanders
Yinghua Chen	Jing Li	Christelle Scharff
Zhenbang Chen	Li Xiaoshan	Marc Segelken
Gabriel Ciobanu	Huimin Lin	Quirico Semeraro
Robert Colvin	Xiang Ling	Kaisa Sere
Pascal Coupey	Daguang Liu	Arne Skou
Werner Damm	Wanwei Liu	Paola Spoletini
Dang Van Hung	Xinxin Liu	Christian Stahl
Rafael del Vado Vírveda	Zhiming Liu	Volker Stolz
Fredrik Degerlund	Jean-Vincent Loddó	K. Subramani
Catalin Dima	Niels Lohmann	Francesco Tiezzi
Wei Dong	Roussanka Loukanova	Tullio Tolio
Brijesh Dongol	Jan Madsen	Marina Waldén
Asger Eir	Tom Maibaum	Ji Wang
Estevez Elsa	Dino Mandrioli	Boris Wirtz
Ignacio Fábregas	Jean-Yves Marion	Jim Woodcock
Dirk Fahland	Peter Massuthe	Peng Wu
John Fisher	Andrea Matta	Zhilin Wu
John Fitzgerald	Alfred Mikschl	Bican Xia
Christophe Fouqueré	Lionel Morel	Lu Yang
Leo Freitas	Peter Mosses	Lu Yang
David Frutos Escrig	Masaki Nakamura	Naijun Zhan
Kokichi Futatsugi	Virginia Niculescu	Huibiao Zhu
Chris George	Thomas Noll	
Michael Reichhardt Hansen	Jens Oehlerking	

Preface

This volume contains the papers presented at the *Festschrift Symposium* held September 24–25, 2007 in Macao on the occasion of the 70th birthdays of Dines Bjørner and Zhou Chaochen. It consists of 25 papers written by 59 authors. Online conference management was provided by EASYCHAIR.

It is now difficult to remember exactly when it came to us that we should organise a celebration for the 70th birthdays of Dines Bjørner and Zhou Chaochen, which happily coincide this year. But I do know that the idea was a popular one. Zhiming Liu suggested that we should organise the symposium as part of the International Colloquium on Theoretical Aspects of Computing, which seemed perfect given that this series was founded by UNU/IIST. The event quickly took shape as He Jifeng offered to host a Training School in Shanghai with the assistance of Chris George, Geguang Pu, and Yong Zhou, and Cliff Jones agreed to help with the academic organisation of the symposium and the colloquium. Everything then just fell into place, thanks to the excellent help provided by the local organisers in Macao and Shanghai.

The subjects for the lectures for the school were obvious to us all: two topics pioneered by Dines Bjørner and Zhou Chaochen, both currently very active research areas. For the *Festschrift Symposium*, authors were invited to write on an original topic of their choosing. And for the colloquium, a general call-for-papers resulted in a satisfying collection of rigorously reviewed papers in theoretical computer science, including automata theory, case studies, concurrency, real-time systems, semantics and logics, and specification and verification.

So we have ended up with three volumes, one each for the school, symposium, and colloquium, which collectively amount to some 1,300 pages. And still there was not enough room for the many additional distinguished names we would have liked to invite.

To Dines and Chaochen from all of us:

We hope that you enjoy reading these books.

Happy birthday to both of you!

June 2007

J.C.P.W.

Organization

Programme Chairs

Cliff Jones
Zhiming Liu
Jim Woodcock

Local Organization

Kitty Chan
Wendy Hoi

Chris George
Violet Pun

Table of Contents

Models and Software Model Checking of a Distributed File Replication System	1
<i>Nikolaj Bjørner</i>	
From “Formal Methods” to System Modeling	24
<i>Manfred Broy</i>	
A Denotational Semantics for Handel-C	45
<i>Andrew Butterfield</i>	
Generating Polynomial Invariants with DISCOVERER and QEPCAD	67
<i>Yinghua Chen, Bican Xia, Lu Yang, and Naijun Zhan</i>	
Harnessing rCOS for Tool Support—The CoCoME Experience	83
<i>Zhenbang Chen, Xiaoshan Li, Zhiming Liu, Volker Stolz, and Lu Yang</i>	
Automating Verification of Cooperation, Control, and Design in Traffic Applications	115
<i>Werner Damm, Alfred Mikschl, Jens Oehlerking, Ernst-Rüdiger Olderog, Jun Pang, André Platzer, Marc Segelken, and Boris Wirtz</i>	
Specifying Various Time Models with Temporal Propositional Variables in Duration Calculus	170
<i>Dang Van Hung</i>	
Relating Domain Concepts Intensionally by Ordering Connections	188
<i>Asger Eir</i>	
Programmable Messaging for Electronic Government - Building a Foundation	217
<i>Elsa Estevez and Tomasz Janowski</i>	
Balancing Insight and Effort: The Industrial Uptake of Formal Methods	237
<i>John Fitzgerald and Peter Gorm Larsen</i>	
Proving Theorems About JML Classes	255
<i>Leo Freitas and Jim Woodcock</i>	
Specification for Testing	280
<i>Chris George, Padmanabhan Krishnan, P.A.P. Salas, and J.W. Sanders</i>	

Semantics and Verification of a Language for Modelling Hardware Architectures	300
<i>Michael R. Hansen, Jan Madsen, and Aske Wiid Brekling</i>	
A Domain-Oriented, Model-Based Approach for Construction and Verification of Railway Control Systems	320
<i>Anne E. Haxthausen and Jan Peleska</i>	
Compensable Programs	349
<i>He Jifeng</i>	
Deriving Specifications for Systems That Are Connected to the Physical World	364
<i>Cliff B. Jones, Ian J. Hayes, and Michael A. Jackson</i>	
Engineering the Development of Embedded Systems	391
<i>Mathai Joseph</i>	
Design Verification Patterns	399
<i>John Knudsen, Anders P. Ravn, and Arne Skou</i>	
On Revival of Algol-Concepts in Modern Programming and Specification Languages	414
<i>Hans Langmaack</i>	
Design in CommUnity with Extension Morphisms	435
<i>Xiang Ling, Tom Maibaum, and Nazareno Aguirre</i>	
Symbolic Test Generation Using a Temporal Logic with Constrained Events	467
<i>Daguang Liu, Peng Wu, and Huimin Lin</i>	
Expansive-Bisimulation for Context-Free Processes	472
<i>Xinxin Liu</i>	
VDM Semantics of Programming Languages: Combinators and Monads	483
<i>Peter D. Mosses</i>	
Formal Approach to Railway Applications	504
<i>Martin Pěnička</i>	
Services as a Paradigm of Computation	521
<i>Wolfgang Reisig, Jan Bretschneider, Dirk Fahland, Niels Lohmann, Peter Massuthe, and Christian Stahl</i>	
Author Index	539