

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

Farhad Arbab Marjan Sirjani (Eds.)

International Symposium on Fundamentals of Software Engineering

International Symposium, FSEN 2007
Tehran, Iran, April 17-19, 2007
Proceedings

Volume Editors

Farhad Arbab
CWI, Leiden University
Kruislaan 413, Amsterdam, The Netherlands
E-mail: Farhad.Arbab@cwi.nl

Marjan Sirjani
University of Tehran, IPM
North Karegar Ave., Tehran, Iran
E-mail: msirjani@ut.ac.ir

Library of Congress Control Number: 2007936606

CR Subject Classification (1998): D.2, D.2.4, F.4.1, D.2.2

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-540-75697-3 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-75697-2 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: 12175260 06/3180 5 4 3 2 1 0

Preface

The present volume contains the post-proceedings of the second IPM International Symposium on Fundamentals of Software Engineering (FSEN), Tehran, Iran, April 17–19, 2007. This event, FSEN 2007, was organized by the School of Computer Science at the Institute for Studies in Fundamental Sciences (IPM) in Iran, in cooperation with the ACM SIGSOFT and IFIP WG 2.2, and was additionally supported by the University of Tehran, Sharif University of Technology, and the International Scientific Meetings Office (ISMO). This symposium brought together researchers and practitioners working on different aspects of formal methods in software engineering. FSEN 2007 covered many aspects of formal methods, especially those related to advancing the application of formal methods in the software industry and promoting their integration with practical engineering techniques.

A truly international program committee of top researchers from 23 different academic institutes in 9 countries selected the technical content of this symposium. We received a total of 73 submissions, out of which the PC selected 22 as regular papers and 8 as short papers to be published in the post-proceedings, and 6 papers accepted for poster presentations at the symposium. Each submission was reviewed by at least 3 independent referees, for its quality, originality, contribution, clarity of presentation, and its relevance to the symposium topics. We had 93 registered participants at the symposium from 12 countries.

We had 4 distinguished keynote speakers at FSEN 2007: James C. Browne, University of Texas at Austin, Texas, USA, on *Unification of Verification and Validation Methods for Software*; Masahiro Fujita, University of Tokyo, Japan, on *Hardware-Software Co-design for SoC with Separated Verification Between Computation and Communication*; Davide Sangiorgi, University of Bologna, Italy, on *Bisimulation in Higher-Order Languages*; and Peter D. Mosses, Swansea University, Wales, UK, on *Fundamentals of Semantics Engineering*.

In conjunction with FSEN 2007, the Working Group 2.2 of IFIP organized 2 full-day tutorials by internationally recognized researchers on the semantics of programming languages (Peter D. Mosses), and the semantics of concurrency (Davide Sangiorgi). These well-attended and well-received tutorials strengthened the impact of FSEN 2007, and we would like to take this opportunity to express our appreciation for the contribution of IFIP WG 2.2 and the tutorial speakers.

We are grateful for the support and the assistance of the IPM staff in the organization of this symposium, especially Dr. Larijani, Dr. Sarbazi-Azad, Ms. Arfai and Mr. Shahrabi. We thank the members of the program committee for their time, effort, and contributions to making FSEN 2007 a quality symposium. Last but not least, our thanks go to our authors and workshop partici-

pants, without whose submissions and participation FSEN 2007 would not have materialized.

April 2007

Farhad Arbab
Marjan Sirjani

Organization

Program Chairs

Farhad Arbab, CWI, Netherlands; Leiden University, Netherlands; University of Waterloo, Canada

Marjan Sirjani, University of Tehran, Iran; IPM, Iran

Program Committee

Gul Agha, University of Illinois at Urbana - Champaign, USA

Farhad Arbab, CWI, Netherlands; Leiden University, Netherlands; University of Waterloo, Canada

Mohammad Ardeshtir, Sharif University of Technology, Iran

Christel Baier, University of Bonn, Germany

Frank S. de Boer, CWI, Netherlands; Leiden University, Netherlands

Marcello Bonsangue, Leiden University, Netherlands

Mario Bravetti, University of Bologna

James C. Browne, University of Texas at Austin, USA

Michael Butler, University of Southampton, UK

Nancy Day, University of Waterloo, Canada

Masahiro Fujita, University of Tokyo, Japan

Maurizio Gabbrielli, University of Bologna, Italy

Jan Friso Groote, Technical University of Eindhoven, Netherlands

Radu Grosu, State University of New York at Stony Brook, USA

Michael Huth, Imperial College of London, UK

Joost Kok, Leiden University, Netherlands

Marta Kwiatkowska, University of Birmingham, UK

Mohammad Reza Meybodi, AmirKabir University of Technology, Iran

Seyed-Hassan Mirian-Hosseiniabadi, Sharif University of Technology, Iran

Ugo Montanari, University of Pisa, Italy

Mohammad Reza Mousavi, Technical University of Eindhoven, Netherlands

Ali Movaghar, IPM, Iran; Sharif University of Technology, Iran

Andrea Omicini, University of Bologna, Italy

George Papadopoulos, University of Cyprus, Cyprus

Jan Rutten, CWI, Netherlands; Vrije University Amsterdam, Netherlands

Sandeep Shukla, Virginia Tech, USA

Marjan Sirjani, IPM, Iran; University of Tehran, Iran

Carolyn Talcott, SRI International, USA

Local Organization

Hamidreza Shahrabi, IPM, Iran (Chair)

Samira Tasharofi, IPM, Iran; University of Tehran, Iran

Hossein Hojjat, IPM, Iran; University of Tehran, Iran

Referees

Sumit Ahuja	Jan Friso Groote	Niloofar Razavi
Elisabeth Ball	Hossein Hojjat	Michel Reniers
Simonetta Balsamo	Hamed Iravanchi	Abdolbaghi Rezazadeh
Massimo Bartoletti	Mohammad Izadi	Shamim Ripon
Debayan Bhaduri	Mohammad-Mahdi	Jan Rutten
Armin Biere	Jaghouri	Werner Sandmann
Stefano Bistarelli	Kevin Kane	Laura Semini
Frank S. de Boer	Stephanie Kemper	Gaurav Singh
Benedikt Bollig	Ramtin Khosravi	Marjan Sirjani
Maria Paola Bonacina	Minyoung Kim	Colin Snook
Pascal Bouvry	Alexander Knapp	Jeremy Sproston
Pyrros Bratskas	Christian Kohler	Andres Stam
Mario Bravetti	Adam Koprowski	Martin Steffen
Adam Brown	Marcel Kyas	Mark-Oliver Stehr
James Browne	Timo Latvala	Syed Suhaib
Michael Butler	Moreno Marzolla	Meng Sun
Marco Carbone	Deepak Abraham	Sameer Sundresh
Liping Chen	Mathaikutty	Paolo Tacchella
Pericles Leng Cheng	Kirill Mechitov	Edward Turner
Tom Chothia	Seyyed Hassan Mirian	Aimilia Tzanavari
Dave Clarke	Mohammad-Reza	Yaroslav Usenko
Claudio Sacerdoti Cohen	Mousavi	Daniele Veracca
John Colley	Ali Movaghar	Fons Verbeek
David Costa	Gethin Norman	Eric Verbeek
Pieter Cuijpers	Farhad Oroumchian	Erik de Vink
Marco Danelutto	Karel Van Oudheusden	Dimitrios Vogiatzis
Nancy Day	David Parker	Marc Voorhoeve
Wan Fokkink	Nearchos Paspallis	Michael Weber
Matthias Fruth	Hiren Patel	Muck van Weerdenburg
Fatemeh Ghassemi	Bas Ploeger	Marco Wiering
Vittorio Ghini	Jaco van de Pol	Hans Zantema
Cinzia di Giusto	Jose Proenca	

Sponsoring Institutions

ACM Special Interest Group on Software Engineering (SIGSOFT)

International Federation for Information Processing (IFIP WG 2.2)

International Scientific Meetings Office (ISMO)
Iran Telecommunications Research Center (ITRC)
Hi-Tech Industries Center of Iran
Electronic Computing Machine Service Company

University of Tehran
Sharif University of Technology
Centrum voor Wiskunde en Informatica (Center for Mathematics and
Computer Science - CWI)

Table of Contents

Finite Abstract Models for Deterministic Transition Systems: Fair Parallel Composition and Refinement-Preserving Logic	1
<i>Harald Fecher and Immo Grabe</i>	
Slicing Abstractions	17
<i>Ingo Brückner, Klaus Dräger, Bernd Finkbeiner, and Heike Wehrheim</i>	
Nuovo DRM Paradiso: Towards a Verified Fair DRM Scheme	33
<i>M. Torabi Dashti, S. Krishnan Nair, and H.L. Jonker</i>	
Formalizing Compatibility and Substitutability in Communication Protocols Using I/O-Constraint Automata	49
<i>Mahdi Niamanesh and Rasool Jalili</i>	
Is Your Security Protocol on Time ?	65
<i>Gizela Jakubowska and Wojciech Penczek</i>	
Adapting the UPPAAL Model of a Distributed Lift System	81
<i>Wan Fokkink, Allard Kakebeen, and Jun Pang</i>	
Zone-Based Universality Analysis for Single-Clock Timed Automata	98
<i>Parosh Aziz Abdulla, Joël Ouaknine, Karin Quaas, and James Worrell</i>	
Compositional Semantics of System-Level Designs Written in SystemC	113
<i>Niloofar Razavi and Marjan Sirjani</i>	
Reusing Requirements: The Need for Extended Variability Models	129
<i>Ramin Tavakoli Kolagari and Mark-Oliver Reiser</i>	
Test Selection Criteria for Quantifier-Free First-Order Specifications	144
<i>Marc Aiguier, Agnès Arnould, Pascale Le Gall, and Delphine Longuet</i>	
Formal Testing of Systems Presenting Soft and Hard Deadlines	160
<i>Mercedes G. Merayo, Manuel Núñez, and Ismael Rodríguez</i>	
Automatic Composition of Stateless Components: A Logical Reasoning Approach	175
<i>Seyyed Vahid Hashemian and Farhad Mavaddat</i>	
A Model of Component-Based Programming	191
<i>Xin Chen, Jifeng He, Zhiming Liu, and Naijun Zhan</i>	

Contract Based Multi-party Service Composition	207
<i>Mario Bravetti and Gianluigi Zavattaro</i>	
Regulating Data Exchange in Service Oriented Applications	223
<i>Alessandro Lapadula, Rosario Pugliese, and Francesco Tiezzi</i>	
A Behavioural Congruence for Web Services	240
<i>Filippo Bonchi, Antonio Brogi, Sara Corfini, and Fabio Gadducci</i>	
Logic-Based Detection of Conflicts in APPEL Policies	257
<i>Carlo Montanero, Stephan Reiff-Marganiec, and Laura Semini</i>	
Hoare Logic for ARM Machine Code	272
<i>Magnus O. Myreen, Anthony C.J. Fox, and Michael J.C. Gordon</i>	
Action Abstraction in Timed Process Algebra: The Case for an Untimed Silent Step	287
<i>Michel A. Reniers and Muck van Weerdenburg</i>	
Type Abstractions of Name-Passing Processes	302
<i>Lucia Acciai and Michele Boreale</i>	
Formal Specification of Multi-agent Systems by Using EUSMs	318
<i>Mercedes G. Merayo, Manuel Núñez, and Ismael Rodríguez</i>	
Strong Safe Realizability of Message Sequence Chart Specifications	334
<i>Abdolmajid Mousavi, Behrouz Far, Armin Eberlein, and Behrouz Heidari</i>	
Implication-Based Approximating Bounded Model Checking	350
<i>Zhenyu Chen, Zhihong Tao, Baowen Xu, and Lifu Wang</i>	
Logical Bisimulations and Functional Languages	364
<i>Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii</i>	
Efficient State Space Reduction for Automata by Fair Simulation	380
<i>Jin Yi and Wenhui Zhang</i>	
Model Checking Temporal Metric Specifications with Trio2Promela	388
<i>Domenico Bianculli, Paola Spoletini, Angelo Morzenti, Matteo Pradella, and Pierluigi San Pietro</i>	
Design and Implementation of a Dynamic-Reconfigurable Architecture for Protocol Stack	396
<i>Mahdi Niamanesh, Sirwah Sabetghadam, Reza Yousefzadeh Rahaghi, and Rasool Jalili</i>	
Vulnerability Analysis in VGBPS using Prolog	404
<i>Mohammad Ebrahim Rafiei, Mohsen Taherian, Hamid Mousavi, Ali Movaghar, and Rasool Jalili</i>	

An Alternative Algorithm for Constraint Automata Product	412
<i>Bahman Pourvatan and Nima Rouhy</i>	
A Review on Specifying Software Architectures Using Extended Automata-Based Models	423
<i>Mehran Sharafi, Fereidoon Shams Aliee, and Ali Movaghar</i>	
ArchC#: A New Architecture Description Language for Distributed Systems	432
<i>Saeed Parsa and Gholamreza Safi</i>	
Relationships Meet Their Roles in Object Oriented Programming	440
<i>Matteo Baldoni, Guido Boella, and Leendert van der Torre</i>	
Author Index	449