

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Lindsay Groves Jing Sun (Eds.)

Formal Methods and Software Engineering

15th International Conference
on Formal Engineering Methods, ICFEM 2013
Queenstown, New Zealand, October 29 – November 1, 2013
Proceedings



Springer

Volume Editors

Lindsay Groves
Victoria University of Wellington
School of Engineering and Computer Science
P.O. Box 600
Wellington 6140, New Zealand
E-mail: lindsay@ecs.vuw.ac.nz

Jing Sun
The University of Auckland
Department of Computer Science
Private Bag 92019
Auckland 1142, New Zealand
E-mail: j.sun@cs.auckland.ac.nz

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-41201-1 e-ISBN 978-3-642-41202-8
DOI 10.1007/978-3-642-41202-8
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013948611

CR Subject Classification (1998): D.2.4, D.2, D.3, F.3, F.4.1, C.2, C.2.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at the 15th International Conference on Formal Engineering Methods (ICFEM 2013) held during 29 October–1 November 2013 in Queenstown, New Zealand.

Since 1997, ICFEM has served as an international forum for researchers and practitioners who have been dedicated to applying formal methods to practical computer systems. This year, we received 88 full paper submissions from 38 different countries. Each paper went through a thorough review process by at least 3 Program Committee members. After extensive discussions, the Committee decided to accept 28 papers, giving the acceptance rate of 31.8%. The proceedings also include the abstracts from 2 keynote speakers.

ICFEM 2013 is organized and sponsored by The University of Auckland. It is the first time that the conference has been held in New Zealand. We acknowledge the financial support received from the Department of Computer Science at The University of Auckland, the Image & Pervasive Access Lab (IPAL) – a French-Singaporean joint research laboratory at National University of Singapore, and the School of Engineering and Computer Science at Victoria University of Wellington. We owe our thanks to the Organizing Committee for their hard work in making ICFEM 2013 a successful event, especially to Sarah Henderson for her technical support to the conference web site.

We are grateful to the Program Committee members and additional reviewers for their support and expertise in completing high quality reviews on time, and most importantly, to all the authors for their contributions to the conference. Finally, we would like to thank the EasyChair conference system, which indeed made the whole process much easier to manage.

July 2013

Lindsay Groves
Jing Sun

Organization

Program Committee

Bernhard K. Aichernig
Yamine Ait Ameer
Keijiro Araki
Farhad Arbab
Richard Banach
Nikolaž Björner
Jonathan Bowen

Michael Butler
Andrew Butterfield
Wei-Ngan Chin
Jim Davies
Jin-Song Dong
Zhenhua Duan
Colin Fidge
John Fitzgerald
Joaquim Gabarro
Stefania Gnesi
Radu Grosu
Lindsay Groves
Ian J. Hayes
Mike Hinchey

Peter Gorm Larsen
Michael Leuschel
Xuandong Li
Yuan-Fang Li
Shang-Wei Lin
Shaoying Liu
Yang Liu
Zhiming Liu

Tiziana Margaria
Hong Mei
Huaikou Miao

Graz University of Technology, Austria
LISI/ENSMA, France
Kyushu University, Japan
CWI and Leiden University, The Netherlands
University of Manchester, UK
Microsoft Research, USA
London South Bank University and Chairman
of Museophile Limited, UK
University of Southampton, UK
Trinity College Dublin, Ireland
National University of Singapore, Singapore
University of Oxford, UK
National University of Singapore, Singapore
Xidian University, China
Queensland University of Technology, Australia
Newcastle University, UK
Universitat Politècnica de Catalunya, Spain
ISTI-CNR, Italy
Stony Brook University, USA
Victoria University of Wellington, New Zealand
University of Queensland, Australia
Lero - the Irish Software Engineering Research
Centre, Ireland
Aarhus School of Engineering, Denmark
University of Düsseldorf, Germany
Nanjing University, China
Monash University, Australia
National University of Singapore, Singapore
Hosei University, Japan
Nanyang Technological University, Singapore
United Nations University - International
Institute for Software Technology, China
University of Potsdam, Germany
Peking University, China
Shanghai University, China

Peter Müller	ETH Zurich, Switzerland
Shin Nakajima	National Institute of Informatics, Japan
Sebastian Nanz	ETH Zurich, Switzerland
Jose Oliveira	Universidade do Minho, Portugal
Jun Pang	University of Luxembourg, Luxembourg
Shengchao Qin	Teesside University, UK
Zongyan Qiu	Peking University, China
Steve Reeves	University of Waikato, New Zealand
Alexander Romanovsky	Newcastle University, UK
Wuwei Shen	Western Michigan University, USA
Marjan Sirjani	Reykjavik University, Iceland
Graeme Smith	University of Queensland, Australia
Jing Sun	The University of Auckland, New Zealand
Jun Sun	Singapore University of Technology and Design, Singapore
Kenji Taguchi	AIST, Japan
Tetsuo Tamai	Hosei University, Japan
Yih-Kuen Tsay	National Taiwan University, China
T.H. Tse	The University of Hong Kong, China
Viktor Vafeiadis	MPI-SWS, Germany
Farn Wang	National Taiwan University, China
Hai H. Wang	University of Aston, UK
Jim Woodcock	University of York, UK
Wang Yi	Uppsala University, Sweden
Jian Zhang	Chinese Academy of Sciences, China
Hong Zhu	Oxford Brookes University, UK
Huibiao Zhu	East China Normal University, China

Additional Reviewers

Arlt, Stephan	Ferrara, Pietro
Bartocci, Ezio	Gao, Honghao
Bendisposto, Jens	Geeraerts, Gilles
Breuer, Peter	He, Guanhua
Bu, Lei	Huang, Yanhong
Carmona, Josep	Iliasov, Alexei
Chen, Liqian	Isobe, Yoshinao
Chen, Yu-Fang	Jafari, Ali
Chen, Zhenbang	Jiao, Li
Ciancia, Vincenzo	Jiao, Wenpin
Costea, Andreea	Khakpour, Narges
Da Cruz, Daniela	Kitamura, Takashi
Dobrikov, Ivo	Kleijn, Jetty
Fantechi, Alessandro	Kong, Weiqiang

Kromodimoeljo, Sentot
Kusakabe, Shigeru
Le, Duy Khanh
Li, Jun
Li, Qin
Lin, Hsin-Hung
Liu, Shuang
Liu, Xuanzhe
Lorber, Florian
Ma, Feifei
Macedo, Hugo
Markovski, Jasen
Omori, Yoichi
Payne, Richard
Pierce, Ken
Rossi, Matteo
Rutten, Eric
Sabouri, Hamideh
Satpathy, Manoranjan
Schäf, Martin
Serrano, Yamilet
Shi, Ling
Snook, Colin
Song, Songzheng

Steffen, Bernhard
Stewart, Alan
Stigge, Martin
Stolz, Volker
Tan, Tian Huat
Thai, Trinh Minh
Trung, Ta Quang
Tsai, Ming-Hsien
Wang, Yasha
Wijs, Anton
Winter, Kirsten
Wu, Xi
Xiong, Yingfei
Yang, Hongli
Yeganeh, Sanaz
Yu, Fang
Zhang, Chenyi
Zhang, Wei
Zhao, Hengjun
Zhao, Jianhua
Zhao, Yongxin
Zheng, Manchun
Zhu, Huiquan
Zhu, Longfei

Keynotes
(Abstracts)

Lattices of Information for Security: Deterministic, Demonic, Probabilistic

Carroll C. Morgan^{*}

School of Computer Science and Engineering
University of New South Wales
`carrollm@cse.unsw.edu.au`

Abstract. Security-oriented analyses of information flow can be in terms of channels (entropy leakage), or in terms of programs (noninterference); and for each we can consider deterministic, demonic or probabilistic instances. We discuss all $2 \times 3 = 6$ cases from a common point of view, seeking a uniform approach to a partial order of information. In some cases this is a lattice (as is already known); and in some cases it seems not to be (novel).

^{*} I am grateful for the support of the Australian Research Council via DP120101413.

Analysis of Continuous Dynamical Systems via Statistical Model Checking

P.S. Thiagarajan

School of Computing, National University of Singapore,
`thiagu@comp.nus.edu.sg`

Abstract. Systems with real-valued variables that evolve continuously w.r.t. time arise in many settings including cyber-physical systems and biochemical networks. The dynamics of these variables will be typically specified in terms of differential equations. An important verification task is to determine whether the global behavior of the system has the required (reachability) properties. The number of the the real-valued variables can be large and their dynamics can be non-linear. For instance, in models of biochemical networks ordinary differential equations are typically used to specify the dynamics. Further, there can be multiple modes of behavior where each mode is governed by a different system of differential equations. Hence the behavior of such systems can seldom be analyzed effectively let alone efficiently.

To get around this we advocate statistical model checking as an *approximate* but scalable analysis technique in these settings. The basic idea is to assume a probability distribution over the initial states of the system. This in turn -under suitable continuity assumptions- induces a distribution over the trajectories generated by the initial states. Hence one can construct a statistical model checking procedure to verify bounded LTL specifications using a simple sequential hypothesis testing method. We demonstrate the applicability of this approach using a number of large biopathways models.

Table of Contents

Keynote

Lattices of Information for Security: Deterministic, Demonic, Probabilistic	1
<i>Carroll C. Morgan</i>	

Specification

Algebraic Laws for Process Subtyping	4
<i>José Dihego, Pedro Antonino, and Augusto Sampaio</i>	
Boundness Issues in CCSL Specifications	20
<i>Frédéric Mallet and Jean-Viven Millo</i>	
Mining Dataflow Sensitive Specifications	36
<i>Zhiqiang Zuo and Siau-Cheng Khoo</i>	

Proof

A Proof Slicing Framework for Program Verification	53
<i>Ton-Chanh Le, Cristian Gherghina, Razvan Voicu, and Wei-Ngan Chin</i>	
Formally Verified System Initialisation	70
<i>Andrew Boyton, June Andronick, Callum Bannister, Matthew Fernandez, Xin Gao, David Greenaway, Gerwin Klein, Corey Lewis, and Thomas Sewell</i>	
Verifying an Aircraft Proximity Characterization Method in Coq	86
<i>Dongxi Liu, Neale L. Fulton, John Zic, and Martin de Groot</i>	

Testing

Assisting Specification Refinement by Random Testing	102
<i>Mengjun Li</i>	
Generation of Checking Sequences Using Identification Sets	115
<i>Faimison Rodrigues Porto, Andre Takeshi Endo, and Adenilso Simao</i>	
The <i>Circus</i> Testing Theory Revisited in Isabelle/HOL	131
<i>Abderrahmane Feliachi, Marie-Claude Gaudel, Makarius Wenzel, and Burkhardt Wolff</i>	

Timed Systems

A CSP Timed Input-Output Relation and a Strategy for Mechanised Conformance Verification	148
<i>Gustavo Carvalho, Augusto Sampaio, and Alexandre Mota</i>	
Deadline Analysis of AUTOSAR OS Periodic Tasks in the Presence of Interrupts	165
<i>Yanhong Huang, João F. Ferreira, Guanhua He, Shengchao Qin, and Jifeng He</i>	
Improving Model Checking Stateful Timed CSP with non-Zenoness through Clock-Symmetry Reduction	182
<i>Yuanjie Si, Jun Sun, Yang Liu, and Ting Wang</i>	

Concurrency

A Modular Approach for Reusing Formalisms in Verification Tools of Concurrent Systems	199
<i>Étienne André, Benoît Barbot, Clément Démoulin, Lom Messan Hillah, Francis Hulin-Hubard, Fabrice Kordon, Alban Linard, and Laure Petrucci</i>	
A UTP Semantics for Communicating Processes with Shared Variables	215
<i>Ling Shi, Yongxin Zhao, Yang Liu, Jun Sun, Jin Song Dong, and Shengchao Qin</i>	
Verification of Static and Dynamic Barrier Synchronization Using Bounded Permissions	231
<i>Duy-Khanh Le, Wei-Ngan Chin, and Yong-Meng Teo</i>	

SysML/MDD

Formal Models of SysML Blocks	249
<i>Alvaro Miyazawa, Lucas Lima, and Ana Cavalcanti</i>	
Towards a Process Algebra Framework for Supporting Behavioural Consistency and Requirements Traceability in SysML	265
<i>Jaco Jacobs and Andrew Simpson</i>	
Translation from Workflow Nets to MSVL	281
<i>Ya Shi, Zhenhua Duan, and Cong Tian</i>	

Verification

Asymptotic Bounds for Quantitative Verification of Perturbed Probabilistic Systems	297
<i>Guoxin Su and David S. Rosenblum</i>	
Verification of Functional and Non-functional Requirements of Web Service Composition	313
<i>Manman Chen, Tian Huat Tan, Jun Sun, Yang Liu, Jun Pang, and Xiaohong Li</i>	
vTRUST: A Formal Modeling and Verification Framework for Virtualization Systems	329
<i>Jianan Hao, Yang Liu, Wentong Cai, Guangdong Bai, and Jun Sun</i>	

Application

Formal Kinematic Analysis of the Two-Link Planar Manipulator	347
<i>Binyameen Farooq, Osman Hasan, and Sohail Iqbal</i>	
Formal Modelling of Resilient Data Storage in Cloud	363
<i>Inna Pereverzeva, Linas Laibinis, Elena Troubitsyna, Markus Holmberg, and Mikko Pöri</i>	
Linking Operational Semantics and Algebraic Semantics for Wireless Networks	380
<i>Xiaofeng Wu and Huibiao Zhu</i>	

Static Analysis

Automated Specification Discovery via User-Defined Predicates	397
<i>Guanhua He, Shengchao Qin, Wei-Ngan Chin, and Florin Craciun</i>	
Path-Sensitive Data Flow Analysis Simplified	415
<i>Kirsten Winter, Chenyi Zhang, Ian J. Hayes, Nathan Keynes, Cristina Cifuentes, and Lian Li</i>	
Reconstructing Paths for Reachable Code	431
<i>Stephan Arlt, Zhiming Liu, and Martin Schäf</i>	
The Domain of Parametric Hypercubes for Static Analysis of Computer Games Software	447
<i>Giulia Costantini, Pietro Ferrara, Giuseppe Maggiore, and Agostino Cortesi</i>	

Author Index	465
-------------------------------	------------