Lecture Notes in Computer Science 8144

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

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

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	Graz University of Technology, Austria
Yamine Ait Ameur	LISI/ENSMA, France
Keijiro Araki	Kyushu University, Japan
Farhad Arbab	CWI and Leiden University, The Netherlands
Richard Banach	University of Manchester, UK
Nikolaj Bjorner	Microsoft Research, USA
Jonathan Bowen	London South Bank University and Chairman of Museophile Limited, UK
Michael Butler	University of Southampton, UK
Andrew Butterfield	Trinity College Dublin, Ireland
Wei-Ngan Chin	National University of Singapore, Singapore
Jim Davies	University of Oxford, UK
Jin-Song Dong	National University of Singapore, Singapore
Zhenhua Duan	Xidian University, China
Colin Fidge	Queensland University of Technology, Australia
John Fitzgerald	Newcastle University, UK
Joaquim Gabarro	Universitat Politecnica de Catalunya, Spain
Stefania Gnesi	ISTI-CNR, Italy
Radu Grosu	Stony Brook University, USA
Lindsay Groves	Victoria University of Wellington, New Zealand
Ian J. Hayes	University of Queensland, Australia
Mike Hinchey	Lero - the Irish Software Engineering Research Centre, Ireland
Peter Gorm Larsen	Aarhus School of Engineering, Denmark
Michael Leuschel	University of Düsseldorf, Germany
Xuandong Li	Nanjing University, China
Yuan-Fang Li	Monash University, Australia
Shang-Wei Lin	National University of Singapore, Singapore
Shaoying Liu	Hosei University, Japan
Yang Liu	Nanyang Technological University, Singapore
Zhiming Liu	United Nations University - International Institute for Software Technology, China
Tiziana Margaria	University of Potsdam, Germany
Hong Mei	Peking University, China
Huaikou Miao	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
Bartocci, Ezio
Bendisposto, Jens
Breuer, Peter
Bu, Lei
Carmona, Josep
Chen, Liqian
Chen, Yu-Fang
Chen, Zhenbang
Ciancia, Vincenzo
Costea, Andreea
Da Cruz, Daniela
Dobrikov, Ivo
Fantechi, Alessandro
Ferrara, Pietro
Gao, Honghao
Geeraerts, Gilles
He, Guanhua
Huang, Yanhong
Iliasov, Alexei
Isobe, Yoshinao
Jafari, Ali
Jiao, Li
Jiao, Wenpin
Khakpour, Narges
Kitamura, Takashi
Kleijn, Jetty
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
Yeganefard, 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

Timed Systems

Concurrency

SysML/MDD

Verification

Application

Static Analysis