Lecture Notes in Computer Science **10009**

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

More information about this series at http://www.springer.com/series/7408

Kazuhiro Ogata · Mark Lawford
Shaoying Liu (Eds.)

Formal Methods and Software Engineering

18th International Conference
on Formal Engineering Methods, ICFEM 2016
Tokyo, Japan, November 14–18, 2016
Proceedings

Springer

Editors
Kazuhiro Ogata
School of Information Science
Japan Advanced Institute of Science and Technology (JAIST)
Nomi
Japan

Mark Lawford
Department of Computing and Software
McMaster University
Hamilton, ON
Canada

Shaoying Liu
Department of Computer Science
Hosei University
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-47845-6 ISBN 978-3-319-47846-3 (eBook)
DOI 10.1007/978-3-319-47846-3

Library of Congress Control Number: 2016954467

LNCS Sublibrary: SL2 – Programming and Software Engineering

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The International Conference on Formal Engineering Methods (ICFEM) is a premier conference for research in all areas related to formal engineering methods, such as verification and validation, software engineering, formal specification and modeling, software security, and software reliability. Since 1997, ICFEM has been serving as an international forum for researchers and practitioners who have been seriously applying formal methods to practical applications. Researchers and practitioners, from industry, academia, and government, are encouraged to attend, present their research, and help advance the state of the art. We are interested in work that has been incorporated into real production systems, and in theoretical work that promises to bring practical and tangible benefit.

In recent years, ICFEM has taken place in Paris, France (2015), Luxembourg (2014), Queenstown, New Zealand (2013), Kyoto, Japan (2012), Durham, UK (2011) and Shanghai, China (2010). The 18^{th} edition of ICFEM took place in Tokyo during November 16–18, 2015. The Program Committee (PC) received 64 full research papers. Each paper received at least three reports from PC members or external reviewers. On the basis of these reports, each submission was extensively discussed in the virtual meeting of the PC, and the PC decided to accept 27 papers. The proceedings also include a full paper and two short summary papers from the three keynote speakers, Tom Maibaum (McMaster University), W. Eric Wong (University of Texas at Dallas), and Keijiro Araki (Kyushu University).

ICFEM 2016 was organized and supported by Hosei University. The conference would not have been possible without the contributions and the support of the following organizations: the Institute of Electronics, Information and Communication Engineers (IEICE), Japan Society for Software Science and Technology (JSSST), and The Murata Science Foundation. We thank also the Local Organizing Committee for their hard work in making ICFEM 2016 a successful and exciting event.

The main event was preceded by three workshops and a tutorial: the 5^{th} International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS 2016), the 6^{th} International Workshop SOFL+MSVL, the Workshop on Formal and Model-Driven Techniques for Developing Trustworthy Systems, and a one day tutorial on formal specification and verification with CafeOBJ.

We would like to thank the numerous people who contributed to the success of ICFEM 2016: the Steering Committee members, the PC members and the additional reviewers for their support in selecting papers and composing the conference program, and the authors and the invited speakers for their contributions without which, of course, these proceedings would not exist. We would like also to thank Springer for

their help during the production of this proceedings volume and the EasyChair team for their great conference system.

August 2016

Kazuhiro Ogata
Mark Lawford
Shaoying Liu

Organization

Program Committee

Bernhard K. Aichernig	TU Graz, Austria
Étienne André	Université Paris 13, France
Toshiaki Aoki	JAIST, Japan
Christian Attiogbe	University of Nantes, France
Richard Banach	University of Manchester, UK
Ezio Bartocci	TU Wien, Austria
Michael Butler	University of Southampton, UK
Ana Cavalcanti	University of York, UK
Sungdeok Cha	Korea University, South Korea
Yuting Chen	Shanghai Jiao Tong University, China
Sylvain Conchon	Université Paris-Sud, France
Frank De Boer	CWI, The Netherlands
Zhenhua Duan	Xidian University, China
Jeremy Gibbons	University of Oxford, UK
Stefania Gnesi	ISTI-CNR, Italy
Lindsay Groves	Victoria University of Wellington, New Zealand
Ian J. Hayes	University of Queensland, Australia
Michaela Huhn	TU Clausthal, Germany
Alexei Iliasov	Newcastle University, UK
Fuyuki Ishikawa	National Institute of Informatics, Japan
Weiqiang Kong	Dalian University of Technology, China
Fabrice Kordon	LIP6/UPMC, France
Mark Lawford	McMaster University, Canada
Xiaoshan Li	University of Macau, SAR China
Shaoying Liu	Hosei University, Japan
Yang Liu	Nanyang Technological University, Singapore
Larissa Meinicke	University of Queensland, Australia
Stephan Merz	Inria Nancy, France
Huaikou Miao	Shanghai University, China
Mohammadreza Mousavi	Halmstad University, Sweden
Shin Nakajima	National Institute of Informatics, Japan
Akio Nakata	Hiroshima City University, Japan
Manuel Nuñez	UC, Spain
Kazuhiro Ogata	JAIST, Japan
Kozo Okano	Shinshu University, Japan
Jun Pang	University of Luxembourg
Jan Peleska	TZI, Universität Bremen, Germany

Ion Petre	Åbo Akademi University, Finland
Shengchao Qin	Teesside University, UK
Silvio Ranise	FBK-Irst, Italy
Adrian Riesco	Universidad Complutense de Madrid, Spain
Jing Sun	University of Auckland, New Zealand
Kenji Taguchi	AIST, Japan
Jaco van de Pol	University of Twente, The Netherlands
Thomas Wahl	Northeastern University, USA
Xi Wang	Hosei University, Japan
Alan Wassyng	McMaster University, Canada
Fatiha Zaidi	Université Paris-Sud, France
Jian Zhang	Institute of Software, Chinese Academy of Sciences, China
Min Zhang	East China Normal University, China
Hong Zhu	Oxford Brookes University, UK
Huibiao Zhu	Software Engineering Institute, East China Normal University, China

Additional Reviewers

Aiguier, Marc
Azadbakht, Keyvan
Basile, Davide
Bloemen, Vincent
Briday, Mikaël
Ciancia, Vincenzo
Colley, John
De Masellis, Riccardo
Dokter, Kasper
Fei, Yuan
Frehse, Goran
Gao, Honghao
Hartmanns, Arnd
He, Mengda
Hoang, Thai Son
Kamali, Mojgan
Khakpour, Narges
Kitamura, Takashi
Konnov, Igor
Kuruma, Hironobu
Laarman, Alfons
Li, Li
Lorber, Florian
Millet, Laure
Oh, Hakjoo
Patcas, Lucian
Petre, Luigia
Renault, Etienne
Ribeiro, Pedro
Salehi Fathabadi, Asieh
Semini, Laura
Souma, Daisuke
Steel, Jim
Su, Wen
Sznajder, Nathalie
Tappler, Martin
Taromirad, Masoumeh
Traverso, Riccardo
Wang, Luyao
Winter, Kirsten
Wu, Xingming
Xu, Zhiwu
Yang, Yilong
Yuan, Qixia
Zheng, Zheng

Abstracts of Keynotes

Combinatorial Testing and Its Applications

W. Eric Wong

Advanced Research Center for Software Testing and Quality Assurance,
Department of Computer Science, University of Texas at Dallas,
Richardson, USA
http://www.utdallas.edu/~ewong
ewong@utdallas.edu

Studies have shown that combinatorial testing can help programs detect hard-to-find software bugs that may not be revealed by test cases generated using other testing techniques. The first part of this talk focuses on traditional black-box requirements-based combinatorial testing. In particular, I will discuss results and lessons learned from two real-life industry applications: a control panel of a rail-road system and a Linux system. The second part extends the concept of combinatorial testing to a white-box structure-based setting. I will present an advanced coverage criterion, *Combinatorial Decision Coverage*, in conjunction with symbolic execution to achieve high coverage cost-effectively without suffering from potential space exploration. Finally, I will explain how combinatorial testing can be applied to a graph-based methodology for testing IoT (Internet of Things).

Bio

W. Eric Wong received his M.S. and Ph.D. in Computer Science from Purdue University, West Lafayette, Indiana, USA. He is a Full Professor, the Director of International Outreach, and the Founding Director of Advanced Research Center for Software Testing and Quality Assurance (http://paris.utdallas.edu/stqa) in Computer Science at the University of Texas at Dallas (UTD). He also has an appointment as a guest researcher at the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce. Prior to joining UTD, he was with Telcordia Technologies (formerly Bellcore) as a senior research scientist and the project manager in charge of Dependable Telecom Software Development.

Dr. Wong is the recipient of the 2014 IEEE Reliability Society Engineer of the Year. He is also the Edit-in-Chief of the IEEE Transactions on Reliability. His research focuses on helping practitioners improve software quality while reducing production cost. In particular, he is working on software testing, program debugging, risk analysis, safety, and reliability. Dr. Wong has published more than 180 papers and edited 2 books.

Dr. Wong is also the Founding Steering Committee Chair of the IEEE International Conference on Software Security and Reliability (SERE) and the IEEE International

Workshop on Program Debugging. In 2015, the SERE conference and the QSIC conference (International Conference on Quality Software) merged into one large conference, QRS, with Q representing *Quality*, R for *Reliability*, and S for *Security*. Dr. Wong continues to be the Steering Committee Chair of this new conference (http://paris.utdallas.edu/qrs).

A (Proto) Logical Basis for the Notion of a Structured Argument in a Safety Case

Valentín Cassano(✉), Thomas S.E. Maibaum, and Silviya Grigorova

McMaster Centre for Software Certification, McMaster University,
Hamilton, Canada.
{cassanv,grigorsb}@mcmaster.ca, tom@maibaum.org

Abstract. The introduction of safety cases was a step in the right direction in regards to safety assurance. As presently practiced, safety cases aim at making a serious attempt to explicate, and to provide some structure for, the reasoning involved in assuring that a system is safe, generally in terms of so-called structured arguments. However, the fact current notations for expressing these structured arguments have no formal semantics and, at best, are loosely linked to goal structuring ideas and to Toulmin's notion of an argument pattern, is a crucial issue to be addressed. History clearly demonstrates that languages that have no formal semantics are deficient in relation to the requirements of a serious approach to engineering. In other words, one can only go so far with intuition, and certainly not far enough to justify the safety of complex systems, such as Cyber Physical Systems or autonomous cars. By rehearsing Gentzen's program for formalizing mathematical reasoning, his famous Calculus of Natural Deduction, we show how we can begin a program of formalizing safety reasoning by developing a working definition of a structured argument in a safety case and a calculus for safety reasoning.

Promotion of Formal Approaches in Japanese Software Industry and a Best Practice of FeliCa's Case (Extended Abstract)

Keijiro Araki[1(✉)] and Taro Kurita[2]

[1] Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
araki@ait.kyushu-u.ac.jp
[2] Sony Corporation, 2-10-1 Osaki, Shinagawa-ku, Tokyo 141-8610, Japan

Abstract. We have been making much effort to promote formal methods in Japan, especially Japanese IT companies. This paper describes our activities in Japan for almost twenty years, and shows typical reactions from such Japanese companies for application of formal methods. We mention about the obstacles they think to adopting formal methods in their real software development projects. On the other hand we also present a case of FeliCa Networks, Inc. as a best practice of applying formal methods in Japan. We discuss the lessons learned from our efforts of promoting formal methods and the FeliCa's case. Finally, we briefly introduce our research project to support software developers in adopting formal approaches to real projects.

Keywords: Formal methods · Rigorous specification · Practice · Development process · FeliCa IC Chip · VDM · VDMPad · ViennaTalk

Contents