

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA


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


Yamine Ait-Ameur · Shengchao Qin (Eds.)

Formal Methods and Software Engineering

21st International Conference
on Formal Engineering Methods, ICFEM 2019
Shenzhen, China, November 5–9, 2019
Proceedings

Editors

Yamine Ait-Ameur 
IRIT/INPT - ENSEEIHT
Toulouse, France

Shengchao Qin 
Teesside University
Middlesbrough, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-32408-7 ISBN 978-3-030-32409-4 (eBook)
<https://doi.org/10.1007/978-3-030-32409-4>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2019

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

The International Conference on Formal Engineering Methods (ICFEM) gathers researchers and practitioners interested in the recent progress in the use and development of formal engineering methods for software and system design. It records the latest development in formal engineering methods.

The 21st edition of ICFEM took place in Shenzhen, China during November 5–9, 2019. ICFEM 2019 received 94 submissions covering theory and applications of formal engineering methods together with case studies. Each paper was reviewed by at least three reviewers and the Program Committee accepted 28 long papers leading to an attractive scientific program.

ICFEM 2019 was marked by the presence of four keynote speakers. The first two talks dealt with machine learning techniques. Yang Liu from Nanyang Technological University, Singapore gave a talk entitled “Secure Deep Learning Engineering: a Road towards Quality Assurance of Intelligent Systems.” The second talk, entitled “Probabilistic Programming for Bayesian Machine Learning,” was given by Luke Ong from Oxford University, United Kingdom. Zhendong Su, from the Swiss Federal Institute of Technology Zurich, Switzerland, gave a talk entitled “Specification-less Semantic Bug Detection” addressing rigorous software bug detection. Finally, with his talk entitled “Taming Delays in Cyber-Physical Systems,” Naijun Zhan from the state key laboratory of Computer Science of the Chinese Academy of Sciences, China addressed formal engineering of Cyber-Physical Systems. The four talks covered current hot research topics. In addition to the mentioned obtained results, these talks revealed many research directions.

After the success of the doctoral symposium of the previous edition, ICFEM 2019 decided to host it again. The doctoral symposium Program Committee chaired by Yi Li from Nanyang Technological University, Singapore and Xin Peng from Fudan University, China accepted eight doctoral papers to be included in the ICFEM 2019 proceedings.

ICFEM 2019 would not have been successful without the deep investment and involvement of the Program Committee members and the external reviewers who contributed by reviewing (with more than 260 reviews) and selecting the best contributions. This event would not exist if authors and contributors did not submit their proposals. We address our thanks to every person, reviewer, author, Program Committee member, and Organization Committee member involved in the success of ICFEM 2019.

The EasyChair system was set up for the management of ICFEM 2019, supporting submission, review, and volume preparation processes. It proved to be a powerful framework.

ICFEM 2019 had three affiliated workshops: the 9th International Workshop on SOFL+MSVL for Reliability and Security (SOFL+MSVL 2019), the 7th International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS 2019), and the

first International Workshop on Artificial Intelligence and Formal Methods (AI&FM 2019). These workshops brought in additional participants to the ICFEM week and helped make it an interesting and successful event. We thank all the workshop organizers and authors for their hard work.

ICFEM 2019 was hosted and sponsored by Shenzhen University, China. The local Organization Committee offered all the facilities to run the conference in a lovely and friendly atmosphere. Many thanks to all the local organizers.

Lastly, we wish to express our special thanks to the general co-chairs Jifeng He and Zhong Ming, and to the Steering Committee members in particular Shaoying Liu and Jin Song Dong for their valuable support.

November 2019

Yamine Ait-Ameur
Shengchao Qin

Organization

Program Committee

Bernhard K. Aichernig	TU Graz, Austria
Yamine Ait Ameer	IRIT/INPT-ENSEEIH, France
Étienne André	Université Paris 13, LIPN, CNRS, UMR 7030, France
Christian Attiogbe	University of Nantes, France
Guangdong Bai	Griffith University, Australia
Christel Baier	TU Dresden, Germany
Richard Banach	The University of Manchester, UK
Luis Barbosa	University of Minho, Portugal
Michael Butler	University of Southampton, UK
Franck Cassez	Macquarie University, Australia
Ana Cavalcanti	University of York, UK
Yuting Chen	Shanghai Jiao Tong University, China
Zhenbang Chen	National University of Defense Technology, China
Wei-Ngan Chin	National University of Singapore, Singapore
Sylvain Conchon	Université Paris-Sud, France
Florin Craciun	Babes-Bolyai University Cluj, Romania
Frank De Boer	CWI, The Netherlands
Yuxin Deng	East China Normal University, China
Jin Song Dong	National University of Singapore, Singapore
Zhenhua Duan	Institute of Computing Theory and Technology, China
Marc Frappier	Université de Sherbrooke, Canada
Stefania Gnesi	ISTI-CNR, Italy
Lindsay Groves	Victoria University of Wellington, New Zealand
Ichiro Hasuo	National Institute of Informatics, Japan
Xudong He	Florida International University, USA
Fuyuki Ishikawa	National Institute of Informatics, Japan
Jie-Hong Roland Jiang	National Taiwan University, Taiwan
Fabrice Kordon	LIP6/Sorbonne Université, CNRS, France
Mark Lawford	McMaster University, Canada
Michael Leuschel	University of Düsseldorf, Germany
Xuandong Li	Nanjing University, China
Yi Li	Nanyang Technological University, Singapore
Yuan-Fang Li	Monash University, Australia
Shaoying Liu	Hosei University, Japan
Shuang Liu	Singapore Institute of Technology, Singapore
Yang Liu	Nanyang Technological University, Singapore
Zhiming Liu	Southwest University, China
Brendan Mahony	Defence Science and Technology Group, Australia

Jim McCarthy	Defence Science and Technology Group, Australia
Dominique Mery	Université de Lorraine, Loria, France
Stephan Merz	Inria Nancy, France
Mohammadreza Mousavi	University of Leicester, UK
Cesar Munoz	NASA, USA
Shin Nakajima	National Institute of Informatics, Japan
Jun Pang	University of Luxembourg, Luxembourg
Yu Pei	The Hong Kong Polytechnic University, SAR China
Xin Peng	Fudan University, China
Geguang Pu	East China Normal University, China
Shengchao Qin	Teesside University, UK
Silvio Ranise	FBK-Irst, Italy
Elvinia Riccobene	University of Milan, Italy
Adrian Riesco	Universidad Complutense de Madrid, Spain
Klaus-Dieter Schewe	Zhejiang University, China
Jing Sun	The University of Auckland, New Zealand
Jun Sun	Singapore Management University, Singapore
Meng Sun	Peking University, China
Cong Tian	Xidian University, China
Elena Troubitsyna	KTH Royal Institute of Technology, Sweden
Jaco van de Pol	Aarhus University, Denmark
Hai H. Wang	University of Aston, UK
Virginie Wiels	ONERA/DTIM, France
Zhiwu Xu	Shenzhen University, China
Naijun Zhan	Chinese Academy of Sciences, China
Jian Zhang	Chinese Academy of Sciences, China
Huibiao Zhu	East China Normal University, China
Peter Ölveczky	University of Oslo, Norway

Additional Reviewers

An, Jie	Dima, Cătălin
Araujo, Hugo	Dong, Yunwei
Basile, Davide	Dong, Zhijiang
Borde, Etienne	Du, Dehui
Bournat, Marjorie	Feliu Gabaldon, Marco Antonio
Braghin, Chiara	Ferrarotti, Flavio
Bu, Lei	Gazda, Maciej
Cai, Chenghao	González, Senén
Cheng, Zheng	Guan, Ji
Chien, Po-Chun	H. Pham, Long
Chondamrongkul, Nacha	He, Chunhui
Ciancia, Vincenzo	He, Mengda
Ciobanu, Gabriel	Hiep, Hans Dieter

Laarman, Alfons

Li, Jiaying

Liyun, Dai

Ma, Feifei

Masci, Paolo

Miao, Weikai

Monin, Jean-Francois

Omitola, Tope

Safey El Din, Mohab

Shi, Ling

Song, Yahui

Sun, Weidi

Tang, Enyi

Vandin, Andrea

Vistbakka, Inna

Waga, Masaki

Wang, Fan

Wang, Qing

Wang, Shuling

Yu, Nengkun

Zhan, Bohua

Zhang, Yuanrui

Zhang, Yueling

Zhao, Hengjun

Zhao, Liang

Zhao, Yongxin

Zuo, Zhiqiang

Abstracts of Invited Talks

Probabilistic Programming for Bayesian Machine Learning

Luke Ong

University of Oxford
`Luke.Ong@cs.ox.ac.uk`

Abstract. Probabilistic programming is a general-purpose means of expressing probabilistic models as computer programs, and automatically performing Bayesian inference such as posterior probability and marginalisation. By providing implementations of these generic inference algorithms, probabilistic programming systems enable data scientists and domain experts to focus on what they can do best, i.e., utilising their domain knowledge to design good models; the task of constructing efficient inference engines can be left to researchers with expertise in statistical machine learning and programming languages. By promoting the separation between model construction and inference procedures, probabilistic programming can democratise access to Bayesian machine learning, with potentially huge benefits to AI and scientific modelling. Because of their generality, probabilistic programming poses interesting and challenging research problems for (both pragmatic and semantic aspects of) programming languages, Bayesian statistics, and machine learning.

In this talk I will introduce probabilistic programming for Bayesian machine learning as a general concept, and explain a number of research directions unique to probabilistic programming.

Specification-Less Semantic Bug Detection

Zhendong Su

Swiss Federal Institute of Technology – ETHZ, Zurich, Switzerland
zhendong.su@inf.ethz.ch

Abstract. The lack of specifications has been the most difficult practical and technical obstacle to software reliability. Without detailed application-specific properties, one cannot utilize formal verification and is confined to detecting generic bugs such as program crashes and memory safety violations, rather than deeper semantic bugs. Breaking this paradoxical impasse is very difficult, and impossible in general. This talk shows how to mitigate it via effective techniques for constructing tests with expected results, thus tackling both test and oracle generation. It illustrates this view with recent successful attacks on difficult testing and analysis problems from diverse domains, ranging from compilers, database engines, to deep learning systems. The talk discusses

1. the high-level principles and core techniques,
2. their significant practical successes—hundreds and thousands of confirmed/fixed bugs in the most widely-used software, and
3. future opportunities and challenges.

Taming Delays in Cyber-Physical Systems

Naijun Zhan

State Key Lab. of Comput. Sci., Institute of Software, CAS
znj@ios.ac.cn

Extended Abstract

Historical motivation (predating digital control):

“Despite [...] very satisfactory state of affairs as far as [ordinary] differential equations are concerned, we are nevertheless forced to turn to the study of more complex equations. Detailed studies of the real world impel us, albeit reluctantly, to take account of the fact that the rate of change of physical systems depends not only on their present state, but also on their past history.”

[Richard Bellman and Kenneth L. Cooke, 1963, see [1]]

Conventional embedded systems have over the past two decades vividly evolved into an open, interconnected form that integrates capabilities of computing, communication and control, thereby triggering yet another round of global revolution of the information technology. This form, now known as cyber-physical systems (CPS), has witnessed an increasing number of safety-critical systems particularly in major scientific projects vital to people’s livelihood. Prominent examples include automotive electronics, health care, nuclear reactors, high-speed trains, aircrafts, spacecrafts, etc., in which a malfunction of any software or hardware component would potentially lead to catastrophic consequences. Meanwhile with the rapid development of feedback control, sensor techniques and computer control, time delays have become an essential feature underlying both the continuous evolution of physical plants and the discrete transition of computer programs, which may well annihilate the stability/safety certificate and control performance of embedded systems. Traditional engineering methods, e.g., testing and simulations, are nevertheless argued insufficient for the zero-tolerance of failures incurred in time-delayed systems in a safety-critical context. Therefore, how to rigorously verify and design reliable safety-critical embedded systems involving delays tends to be a grand challenge in computer science and the control community.

In contrast to delay-free systems, time-delayed systems yield substantially higher theoretical complexity thus rendering the underlying design and verification tasks exceedingly harder, e.g., unlike Ordinary Differential Equations (ODEs) being

Markovian process, Delay Differential Equations (DDEs) turn out to be non-Markovian, heavily depending on their execution histories, and consequently any solution to a DDE is an infinite dimensional functional, rather than a point in the n -dimensional Hilbert space like ODE's. The major problems that we faced include the formal verification and controller synthesis of time-delayed, networked hybrid systems.

Though time delays have been extensively studied in the literature of mathematics and control theory from a qualitative perspective, automatic verification and synthesis methods addressing feedback delays in hybrid discrete-continuous systems are still in their infancy. In this extended abstract, we summarize our recent efforts towards the above issues, including

- Firstly, we will discuss how to synthesize controllers for time-delayed discrete systems, based on the work in [3]. The basic idea is to reduce the controller synthesis problem to a two-player delay safety game, further to a two-player delay-free safety game with memory. Based on the reduction, an efficient incremental synthesis algorithm is presented. According to the work in [4], we further discuss generalized settings of controller synthesis where messages may arrive out of order or even get lost, and show –on top of the incremental synthesis– the equivalence of qualitative controllability over these settings.
- Then, we discuss bounded reachability analysis of DDEs, mainly focusing on two approaches: the first one is to extend the technique of *simulation plus sensitivity analysis* for ODEs [6] to DDEs [2]; the other is to extend the set-boundary reachability analysis methods for ODEs [8] to DDEs [7].
- Finally, we discuss unbounded verification of DDEs, mainly focusing on the following two approaches: the first one is to deal with DDEs of the form

$$\frac{d}{dt}x(t) = f(x(t - \delta))$$

by exploiting *interval Taylor models* and *stability analysis*. The basic idea can be sketched as follows:

1. predefine a parametric interval polynomial containing all possible solutions of the DDE on the given segment,
2. derive an operator between the parameters of the solution on the previous segment and the ones on the next segment, forming a time-invariant discrete dynamical system,
3. exploit the stability analysis of the resulted time-invariant dynamical system, thus reducing the safety verification and stability analysis to bounded cases.

The detail can be found in [9]; the other approach is to deal with the general DDEs of the form

$$\frac{d}{dt}x(t) = f(x(t), x(t - \delta_1), \dots, x(t - \delta_n))$$

by using *linearisation* and *spectral analysis*. The reader can refer to [5] for the detail. The basic idea can be sketched as follows:

1. linearise a non-linear DDE,
2. exploit spectral analysis to obtain the stability of the linear part,
3. reduce unbounded verification and analysis to bounded case.

Finally, we will also discuss trends and challenges in the formal verification and synthesis of time-delayed systems.

Acknowledgements. First of all, I thank Mingshuai Chen and Bai Xue for their useful comments on the early version of the manuscript which improve the presentation so much.

I would like to take this opportunity to thank all collaborators involved in this research, including Martin Fränzle, Bai Xue, Liang Zou, Mingshuai Chen, Peter Nazier Mosaad, Yangjia Li, Shenghua Feng, etc.

References

1. Bellman, R., Cooke, K.L.: Differential-difference equations. Technical report R-374-PR, The RAND Corporation, Santa Monica, California, January 1963
2. Chen, M., Fränzle, M., Li, Y., Mosaad, P.N., Zhan, N.: Validated simulation-based verification of delayed differential dynamics. In: Fitzgerald, J., Heitmeyer, C., Gnesi, S., Philippou, A. (eds.) FM 2016. LNCS, vol. 9995, pp 137–154. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-48989-6_9
3. Chen, M., Fränzle, M., Li, Y., Mosaad, P.N., Zhan, N.: What’s to come is still unsure - synthesizing controllers resilient to delayed interaction. In: Lahiri, S., Wang, C. (eds.) ATVA 2018. LNCS, vol. 11138, pp. 56–74. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-48989-6_9
4. Chen, M., Fränzle, M., Li, Y., Mosaad, P.N., Zhan, N.: Indecision and delays are the parents of failure: taming them algorithmically by synthesizing delay-resilient control. Acta Informatica (2019). Under minor revision
5. Feng, S., Chen, M., Zhan, N., Fränzle, M., Xue, B.: Taming delays in dynamical systems: unbounded verification of delay differential equations. In: Dillig, I., Tasiran, S. (eds.) CAV 2019. LNCS, vol. 11561, pp. 650–669. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25540-4_37
6. Nahhal, T., Dang, T.: Test coverage for continuous and hybrid systems. In: Damm, W., Hermanns, H. (eds.) CAV 2007. LNCS, vol. 449–462. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73368-3_47
7. Xue, B., Mosaad, P.N., Fränzle, M., Chen, M., Li, Y., Zhan, N.: Safe over- and under-approximation of reachable sets for delay differential equations. In: Abate, A., Geeraerts, G. (eds.) FORMATS 2017. LNCS, vol. 10419, pp. 281–299. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-65765-3_16
8. Xue, B., She, Z., Easwaran, A.: Under-approximating backward reachable sets by polytopes. In: Chaudhuri, S., Farzan, A. (eds.) CAV 2016. LNCS, vol. 9779, pp. 457–476. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41528-4_25
9. Zou, L., Fränzle, M., Zhan, N., Mosaad, P.N.: Automatic verification of stability and safety for delay differential equations. In: Kroening, D., Păsăreanu, C. (eds.) CAV 2015. LNCS, vol. 9207, pp. 338–355. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21668-3_20

Secure Deep Learning Engineering: A Road Towards Quality Assurance of Intelligent Systems

Yang Liu

Nanyang Technological University, Singapore, Singapore
yangliu@ntu.edu.sg

Abstract. Over the past decades, deep learning (DL) systems have achieved tremendous success and gained great popularity in various applications, such as intelligent machines, image processing, speech processing, and medical diagnostics. Deep neural networks are the key driving force behind its recent success, but still seem to be a magic black box lacking interpretability and understanding. This brings up many open safety and security issues with enormous and urgent demands on rigorous methodologies and engineering practice for quality enhancement. A plethora of studies have shown that state-of-the-art DL systems suffer from defects and vulnerabilities that can lead to severe loss and tragedies, especially when applied to real-world safety-critical applications.

In this paper, we perform a large-scale study and construct a paper repository of 223 relevant works to the quality assurance, security, and interpretation of deep learning. Based on this, we, from a software quality assurance perspective, pinpoint challenges and future opportunities to facilitate drawing the attention of the software engineering community towards addressing the pressing industrial demand of secure intelligent systems.

Contents

Invited Talk

Secure Deep Learning Engineering: A Road Towards Quality Assurance of Intelligent Systems	3
<i>Yang Liu, Lei Ma, and Jianjun Zhao</i>	

Regular Papers

Using DimSpec for Bounded and Unbounded Software Model Checking	19
<i>Marko Kleine Büning, Tomáš Balyo, and Carsten Sinz</i>	
SMTBCF: Efficient Backbone Computing for SMT Formulas	36
<i>Yueling Zhang, Geguang Pu, and Min Zhang</i>	
Automatic Verification for Node-Based Visual Script Notation Using Model Checking	52
<i>Isamu Hasegawa and Tomoyuki Yokogawa</i>	
A Reo Model of Software Defined Networks	69
<i>Hui Feng, Farhad Arbab, and Marcello Bonsangue</i>	
Design of Point-and-Click User Interfaces for Proof Assistants	86
<i>Bohua Zhan, Zhenyan Ji, Wenfan Zhou, Chaozhu Xiang, Jie Hou, and Wenhui Sun</i>	
SqlSol: An accurate SQL Query Synthesizer.	104
<i>Lin Cheng</i>	
Towards Verifying Ethereum Smart Contracts at Intermediate Language Level	121
<i>Ximeng Li, Zhiping Shi, Qianying Zhang, Guohui Wang, Yong Guan, and Ning Han</i>	
Simulations for Multi-Agent Systems with Imperfect Information	138
<i>Patrick Gardy and Yuxin Deng</i>	
On the Generation of Equational Dynamic Logics for Weighted Imperative Programs	154
<i>Leandro Gomes, Alexandre Madeira, Manisha Jain, and Luis S. Barbosa</i>	
A Security Calculus for Wireless Networks of Named Data Networking	170
<i>Yuan Fei, Huibiao Zhu, Haiying Sun, and Jiaqi Yin</i>	

Automatic Modularization of Large Programs for Bounded Model Checking	186
<i>Marko Kleine Büning and Carsten Sinz</i>	
PDNet: A Programming Language for Software-Defined Networks with VLAN	203
<i>Shuangqing Xiang, Marcello Bonsangue, and Huibiao Zhu</i>	
Consistency Enforcement for Static First-Order Invariants in Sequential Abstract State Machines.	219
<i>Klaus-Dieter Schewe</i>	
Probably Approximate Safety Verification of Hybrid Dynamical Systems. . . .	236
<i>Bai Xue, Martin Fränzle, Hengjun Zhao, Naijun Zhan, and Arvind Easwaran</i>	
A Formally Verified Algebraic Approach for Dynamic Reliability Block Diagrams	253
<i>Yassmeen Elderhalli, Osman Hasan, and Sofiène Tahar</i>	
Reasoning About Universal Cubes in MCMT.	270
<i>Sylvain Conchon and Mattias Roux</i>	
sCompile: Critical Path Identification and Analysis for Smart Contracts	286
<i>Jialiang Chang, Bo Gao, Hao Xiao, Jun Sun, Yan Cai, and Zijiang Yang</i>	
A Mechanized Theory of Program Refinement	305
<i>Boubacar Demba Sall, Frédéric Peschanski, and Emmanuel Chailloux</i>	
A Relational Static Semantics for Call Graph Construction.	322
<i>Xilong Zhuo and Chenyi Zhang</i>	
Solution Enumeration Abstraction: A Modeling Idiom to Enhance a Lightweight Formal Method.	336
<i>Allison Sullivan, Darko Marinov, and Sarfraz Khurshid</i>	
Formal Analysis of Qualitative Long-Term Behaviour in Parametrised Boolean Networks.	353
<i>Nikola Beneš, Luboš Brim, Samuel Pastva, Jakub Poláček, and David Šafránek</i>	
Combining Parallel Emptiness Checks with Partial Order Reductions.	370
<i>Denis Poitrenaud and Etienne Renault</i>	
A Coalgebraic Semantics Framework for Quantum Systems	387
<i>Ai Liu and Meng Sun</i>	

Parameterized Hardware Verification Through a Term-Level Generalized Symbolic Trajectory Evaluation	403
<i>Yongjian Li and Bow-yaw Wang</i>	
An Axiomatisation of the Probabilistic μ -Calculus.	420
<i>Junnan Xu, Wanwei Liu, David N. Jansen, and Lijun Zhang</i>	
Synthesizing Nested Ranking Functions for Loop Programs via SVM	438
<i>Yi Li, Xuechao Sun, Yong Li, Andrea Turrini, and Lijun Zhang</i>	
A First Step in the Translation of Alloy to Coq	455
<i>Salwa Souaf and Frédéric Loulergue</i>	
Assessment of a Formal Requirements Modeling Approach on a Transportation System	470
<i>Steve Jeffrey Tueno Fotso, Régine Laleau, Marc Frappier, Amel Mammam, Francois Thibodeau, and Mama Nsangou Mouchili</i>	
Doctoral Symposium Papers	
Design Model Repair with Formal Verification.	489
<i>Cheng-Hao Cai, Jing Sun, and Gillian Dobbie</i>	
A Performance-Sensitive Malware Detection System on Mobile Platform. . . .	493
<i>Ruitao Feng, Yang Liu, and Shangwei Lin</i>	
Certifying Hardware Model Checking Results.	498
<i>Zhengqi Yu, Armin Biere, and Keijo Heljanko</i>	
A Note on Failure Mode Reasoning	503
<i>Hamid Jahanian</i>	
Robustness of Piece-Wise Linear Neural Network with Feasible Region Approaches	507
<i>Jay Hoon Jung and YoungMin Kwon</i>	
Formal Specification and Verification of Smart Contracts.	512
<i>Jiao Jiao</i>	
Spatio-Temporal Specification Language for Cyber-Physical Systems	517
<i>Tengfei Li</i>	
A Modeling Framework of Cyber-Physical-Social Systems with Human Behavior Classification Based on Machine Learning.	522
<i>Dongdong An, Jing Liu, Xiaohong Chen, Tengfei Li, and Ling Yin</i>	
Author Index	527