Xie T, Qin S, Zhang W. Special section on software systems 2021—Theme: Dependable software engineering. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 36(6): 1229–1230 Nov. 2021. DOI 10.1007/s11390-021-0008-x

Preface

As a continuation of previous years' special section on software systems, this special section encourages and promotes research to address challenges from the perspective of software systems. The goal of this special section is to present state-of-the-art and high-quality original research in the area of software systems.

The theme of this special section is **Dependable Software Engineering**. This theme encompasses all the research challenges that concern software quality achieved through formal methods, software testing and analysis techniques that contribute to the development of dependable software. The ever increasing diversity, ubiquity, and dynamism of modern software systems are making the development of dependable software more challenging.

The special section received 14 submissions. Many of them are of highly competitive quality. After the thorough review and revision process, we had to make very difficult decisions to accept 10 submissions, of which eight are included in this special section and two are planned to be included in an upcoming issue.

The article "A Multi-Agent Spatial Logic for Scenario-Based Decision Modeling and Verification in Platoon Systems" by Xu *et al.* proposes a formal modeling and verification approach to provide safety assurance for platoon vehicles' cooperative driving behaviors, by extending the multi-agent spatial logic (MASL) with relative orientation and multi-agent observation and utilizing a timed automata type supporting MASL formulas to model vehicles' decision controllers for platoon driving, of which the viability has been demonstrated by a case study in which safety properties of a human-driven vehicle joining the platoon are verified with the use of UPPAAL.

The article "MEBS: Uncovering Memory Life-Cycle Bugs in Operating System Kernels" by Zhang *et al.* presents a study of memory life-cycle bugs and an implementation of a memory life-cycle bug sanitizer (MEBS) with the use of inter-procedural global call graphs for bug detection that may reveal memory allocation, dereferencing, and freeing sites in kernels, of which the effectiveness has been demonstrated by experimental results on operating system kernels.

The article "Trace Semantics and Algebraic Laws for Total Store Order Memory Model" by Xiao *et al.* investigates the trace semantics and algebraic laws for the total store order, a widely-used weak memory model in SPARC implementations and x86 architecture, by applying the unifying theories of programming, and the link between the trace semantics and the algebraic semantics has been established through deriving trace semantics from algebraic semantics.

The article "Symbolic Reasoning About Quantum Circuits in Coq" by Shi *et al.* proposes a symbolic approach to reasoning about quantum circuits based on a set of laws involving basic manipulations on vectors and matrices, with the advantage that it scales better than the explicit one and is well suited to be automated in Coq, as demonstrated with typical examples.

The article "HRPDF: A Software-Based Heterogeneous Redundant Proactive Defense Framework for Programmable Logic Controller" by Liu *et al.* proposes a programmable logic controller (PLC) compatible software-based defense mechanism for thwarting multiple types of attacks against PLCs without the need of external devices, of which a prototype system has been implemented and evaluated in a real-world PLC and an OpenPLC-based device.

The article "AMCheX: Accurate Analysis of Missing-Check Bugs for Linux Kernel" by Wang *et al.* proposes a missing-check analysis method for the Linux kernel for automatically inferring possible security-sensitive operations, and based on the proposed method, a tool named AMCheX has been implemented on top of the LLVM framework and the effectiveness of the tool has been demonstrated by an application on the Linux kernel.

The article "Verifying Contextual Refinement with Ownership Transfer" by Li and Feng proposes an approach to give abstract and implementation independent specifications to concurrent objects with ownership transfer by designing a program logic to verify contextual refinement of concurrent objects w.r.t. their abstract specifications, of which the applicability has been demonstrated by verifying a simplified version of the memory management module of a real-world preemptive OS kernel.

The article "Verification of Real Time Operating System Exception Management Based on SPARCv8" by Ma *et al.* proposes a Hoare-style framework to verify the exception management based on SPARCv8 (Scalable Processor Architecture Version 8) processor architecture at the design layer, of which the application has been demonstrated by verifying the exception management of the real-time operating system SpaceOS on the Beidou-3 satellite, with the use of the interactive theorem prover Coq.

We thank all the authors who submitted to this special section. We appreciate great help from the guest editors: Shengchao Qin (Huawei Hong Kong Research Centre, Hong Kong) and Wenhui Zhang (Institute of Software, Chinese Academy of Sciences, Beijing). We are also highly appreciative to the reviewers who provided valuable review feedback on the submissions in a tight schedule. All these preceding contributions make this special section possible.

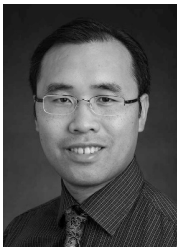
Leading Editor:

Tao Xie, Chair Professor, School of Computer Science, Peking University, Beijing taoxie@pku.edu.cn

Guest Editors:

Shengchao Qin, Senior Software Expert, Huawei Hong Kong Research Centre, Hong Kong
shengchao.qin@gmail.com

Wenhui Zhang, Professor, Institute of Software, Chinese Academy of Sciences, Beijing zwh@ios.ac.cn



Tao Xie is a chair professor in the School of Computer Science at Peking University, Beijing. He received his Ph.D. degree in computer science from the University of Washington at Seattle in 2005. He received his M.S. degree in computer science from Peking University, Beijing, in 2000, and his B.S. degree in computer science from Fudan University, Shanghai, in 1997. His research interests are in software engineering, system software, software security, and trustworthy AI. He is an AAAS Fellow, ACM Distinguished Scientist, IEEE Fellow, and a distinguished member of CCF.

Shengchao Qin is currently a senior software expert in Huawei Hong Kong Research Centre, Hong Kong. He got his Ph.D. degree in applied mathematics from Peking University, Beijing, and also worked as a Postdoctoral Research Fellow in National University of Singapore under the Singapore-MIT Alliance program, before moving his job to UK. While in UK, he worked as a university lecturer in Durham University, and reader in Teesside University, before being promoted to professor (chair) of Computer Science in 2011. He also acted as associate dean for Research and Innovation between 2016 and 2019. His research interests lie mainly in formal methods, software engineering and programming languages, in particular, formal specification and modelling, program analysis and verification, theories of programming, and program logic such as separation logic. To this date he has published over 130 papers in international journals and peer-refereed international conferences. He is a senior member of both ACM and IEEE. He serves as a full member of EPSRC peer review college and a member of UKRI Future Leaders Fellowship peer review college.

Wenhui Zhang is a professor at the Institute of Software of the Chinese Academy of Sciences, Beijing. He had studied at the Department of Mathematics of Peking University, Beijing, and at the Department of Informatics of the University of Oslo, Oslo, and received his Ph.D. degree from the latter in 1988. Prior to joining the Institute of Software in 2001, he was a research scientist at the Institute of Energy Technology, Halden, Norway. His current research interests include formal methods, logics and semantics, deductive and automated proof methods, and software verification techniques.