International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2021, 11(4): 379–381, doi: 10.21655/ijsi.1673-7288.00252

Preface

Preface to the Topic of Formal Methods and Their Applications

Cong Tian (田聪)[1], Yuxin Deng (邓玉欣)[2], Yu Jiang (姜宇)[3]

[1] (School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi 710071, China)
[2] (Software Engineering Institute, East China Normal University, Shanghai 200062, China)
[3] (School of Software, Tsinghua University, Beijing 100084, China)
Corresponding author: Tian Cong, ctian@mail.xidian.edu.cn; Deng Yuxin, yxdeng@sei.ecnu.edu.cn; Jiang Yu, jiangyu198964@126.com

Citation Tian C, Deng YX, Jiang Y. Preface to the topic of formal methods and their applications, *International Journal of Software and Informatics*, 2021, 11(4): 379–381. http://www.ijsi.org/1673-7288/252.htm

The progress of computer science involves the development of hardware and software, one core problem of which is how to ensure their security and reliability. The constant improvement of hardware performance and computing speed, coupled with the increasingly complex system architecture and software functions, makes it difficult to develop secure and reliable software and hardware systems, posing a grand challenge to the development of computer science. As computer systems are widely used in many safety-critical systems, such as high-speed train control system, aerospace control system, and medical equipment control system, the errors in these computer systems may lead to disastrous consequences.

As an important means to improve the security and reliability of software systems, formal methods have been successfully applied to the design of hardware products, especially semiconductor chips. Every major hardware manufacturer such as IBM and AMD has a competent research team of formal methods responsible for providing technical support to ensure system reliability. With the advancement of formal verification techniques and tools in recent years, especially their successful application in program verification, formal methods have demonstrated unparalleled potential in dealing with the complexity of software development and improving software reliability. Many famous research institutions have invested massive human and material resources in this field. For example, the formal methods research team of NASA has played an important role in ensuring the USA correctness of the spacecraft control software. During the process of developing the Curiosity Mars rover, formal methods were used intensively to improve the reliability and efficiency of the control software. In addition, formal methods provide theoretical guarantee and effective solutions in software analysis, malicious code detection and so on. They have been increasingly used in some emerging fields such as blockchain and artificial intelligence, playing a significant role in ensuring the security and credibility of AI applications and improving the overall security and controllability of the system.

This special issue focuses on the latest progress of formal methods and related tools, as well as the practical work of ensuring security and reliability of software and hardware systems, including (1) the work proposing, improving and applying formal methods and related tools for

Received 2021-07-12; IJSI published online 2021-12-23

solving new problems and verifying new systems; (2) the research and practical work related to the fusion of formal methods and other emerging technologies like artificial intelligence. Some representative research results are summarized below:

(1) The work proposing, improving and applying formal methods and related tools. Since software has become a kind of social infrastructure, it is necessary to innovate the formal methods so as to suit new forms and important status of software. Therefore, it is essential to propose new formal methods and related tools as well as upgrade the traditional ones. To tackle the problem of determining the coverage of safe Petri nets, a research team at Shandong University of Science and Technology employed a heuristic technique to reduce the scale of expansion and proposed a new target-oriented reverse expansion algorithm, improving the efficiency of coverage determination. The team of the State Key Laboratory of Mathematical Engineering and Advanced Computing proposed a formal verification method for detecting the semantic logic errors of security protocol code, which automatically abstracts the protocol's C source code into a Pi calculus model and performs formal verification on the protocol's security attributes based on the model. A team at Nanjing University of Aeronautics and Astronautics put forward a new definition of matrix equivalence, improved the previous formal work, proved a set of new lemmas, and finally built different types of basic libraries for the formalization of matrices and block matrices.

(2) The description and verification of new problems and systems. In recent years, the functions of software systems have become increasingly powerful and complex. Formal methods and related tools have been applied in many new software systems, especially safety-critical systems. For example, a team at Beijing Institute of Control Engineering proposed a verification framework based on Hoare-logic to prove the correctness of exception management for the operating system running on the SPARC processor architecture. They used this framework to verify the correctness of the exception management functions of SpaceOS, the embedded real-time spacecraft operating system of BDS-3. A team at Nanjing University studied the distributed consensus protocol Raft used in the distributed file system PolarFS and proposed a new version of Raft that supported out-of-order execution. Furthermore, they performed formalized rectification and verification by using the TLA+-related methods and tools, proving the correctness of the protocol. A team at Capital Normal University used the method of probability model testing to conduct formal modeling and analysis for the data flow-oriented data distribution mechanism of ROS2, proving that the ROS2 communication system had high real-time performance and reliability.

(3) The fusion of formal methods with emerging technologies such as artificial intelligence and blockchain. Formal methods are closely related to artificial intelligence. On the one hand, it is feasible to enhance the formal methods with artificial intelligence. On the other hand, it is also of great significance to study the formal methods for machine learning software. Formal methods have also been widely used in other emerging fields such as blockchain. For example, a team at Central South University studied the automatic generation of coarse-grained PR descriptions on the GitHub platform. For the formalization of PR description generation, they made use of graph neural networks and reinforcement learning to generate PR descriptions with good readability. A team at Capital Normal University formalized Yul, an intermediate language of Ethereum. They proposed formal definitions of the type system and small-step operational semantics of Yul by using the proof assistant Isabelle/HOL, laying a foundation for verifying the correctness and security of smart contracts.

In summary, this special issue focuses on the advancement in the frontier of formal methods and their applications, as well as the role formal methods play in guaranteeing the reliability and security of current software and hardware systems, reflecting the high-level achievements

of Chinese scholars in this field. We hope this special issue can provide useful information and promote the research on formal methods.

The following is a list of the 6 representative papers included in this special issue, along with their brief description:

"*Automatic Generation of Large-Granularity Pull Request Description"* proposes a method to automatically generate descriptions for large-granularity pull requests in the GitHub platform. This method models the PR description generation task as the extractive generation of text summary, and uses graph neural networks and reinforcement learning to generate PR description with better readability, achieving the performance superior to the existing PR descriptions generation methods.

"*Reverse Unfolding of Petri Nets and its Application in Program Data Race Detection*" proposes a target-oriented reverse unfolding algorithm for the coverability problem of safe Petri nets. The authors then apply this algorithm to the data race detection in a group of concurrent programs, proving that the reverse unfolding is more efficient than forward unfolding when the Petri net has more forward branches than backward branches.

"*On Schedulability Analysis of AADL Architecture with Storage Resource Constraint*" proposes a model-based architecture level schedulability evaluation and verification method for cache resource constrained. The authors then verify the feasibility of this method with a use case of aircraft airborne open-architecture intelligent information system.

"*Smooth Intervention Model of Individual Interaction Behavior*" proposes a smooth intervention model for individual interactive behavior, which can well guide the smooth change of user behaviors and produce sufficient discrimination, thereby significantly improving the model accuracy in the scenario of behavior camouflage anomaly detection.

"*Raft with Out-of-Order Executions*" proposes a ParallelRaft-SE protocol based on Raft that allows out-of-order commitment but prohibits out-of-order executions, and further proposes a ParallelRaft-CE protocol supporting out-of-order execution. The authors use TLA+ to provide formal specifications of ParallelRaft-SE and ParallelRaft-CE and verify the correctness of the algorithm when the number of participants is small.

"*Modeling and Analysis of ROS2 Data Distribution Service for Data Flow*" proposes ROS2 system with data flow-oriented data distribution service system and adopts the method of probability model test to validate the real-time performance and reliability of the ROS2 system.

Cong Tian, Ph.D., professor and doctoral supervisor at School of Computer Science and Technology, Xidian University, outstanding member of CCF, with the main research fields of formal methods, program verification, etc.

Yu Jiang, Ph.D., associate professor and doctoral supervisor at School of Software, Tsinghua University, CCF member, with the main research fields of formal methods, program analysis, embedded software, etc.

Yuxin Deng, Ph.D., professor and doctoral supervisor at School of Software Engineering, East China Normal University, senior member of CCF, with the main research fields of formal methods, program theory, etc.