International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2023, 13(3): 243–245, doi: 10.21655/ijsi.1673-7288.00299

Preface

Preface to the Special Issue on Constraint Solving and Theorem Proving

Shaowei Cai (蔡少伟)[1], Zhenbang Chen (陈振邦)[2], Ji Wang (王戟)[2],
Bohua Zhan (詹博华)[1], Yongwang Zhao (赵永望)[3]

[1] (Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[2] (School of Computing, National University of Defense Technology, Changsha 410073, China)
[3] (College of Computer Science and Technology, Zhejiang University, Hangzhou 310007, China)
Corresponding author: Shaowei Cai, caisw@ios.ac.cn

Citation Cai SW, Chen ZB, Wang J, Zhan BH, Zhao YW. Preface to the special issue on constraint solving and theorem proving, *International Journal of Software and Informatics*, 2023, 13(3): 243–245. http://www.ijsi.org/1673-7288/299.htm

The security and reliability of software and hardware systems are receiving increasing attention in various fields, such as aerospace and high-speed rail. The formal method models the computer system and verifies the correctness of the system with the help of computers by means of a strict mathematical language. Unlike testing, the formal method approach can eliminate certain types of errors. Constraint solving and theorem proving are two key techniques in formal methods.

Constraint solving mainly refers to SAT solving algorithms and SMT solving algorithms in the field of formal verification, although in a broad sense, constraint solving algorithms also include CSP algorithms and other types of constraint algorithms. The SAT algorithm is applicable for determining the logical relationship between Boolean variables, while SMT can determine logical formulas containing variables of various data types. SAT solvers have many applications in the field of EDA, especially logic synthesis and formal verification. SMT solvers are mainly used for program analysis and software verification.

SAT solving has entered a very mature stage after half a century of study. However, new challenges are constantly posed to this direction with the increasing scale of integrated circuits. The study of the SMT algorithms started relatively late, and it is generally believed that it began around 2000. The existing SMT solvers are mainly developed by teams from top universities and companies in the United States. China has entered the international forefront of SAT solvers in recent years, but its study on SMT solvers still lags behind European and American countries. However, China has also begun to achieve distinctive achievements in certain theories of SMT and has reached the international forefront in corresponding issues.

Theorem proving includes automatic theorem proving and interactive theorem proving. Interactive theorem proving is achieved through the interaction between humans and computers, verifying complex systems and properties, such as the correctness verification of compilers and operating systems. Some complex systems are difficult to be verified through constraint solving and automatic theorem proving, and generally resort to interactive theorem proving.

Received 2023-02-21; Accepted 2023-02-28; IJSI published online 2023-09-27

This special issue focuses on the study of constraint solving and theorem proving in the field of formal methods, including the theory, technology, tools, and applications of constraint solving and theorem proving. The five selected papers are summarized as follows.

UC-based Approximate Incremental Reachability proposes a novel accessibility analysis method based on an invariant solution, which implements an efficient security model checking and verification algorithm by building a series of monotonic candidate invariants to ultimately approximate the real invariants. Experiments have shown that this method complements the performance of existing mature model checking techniques.

GC-MCR: *Directed Graph Constraint-guided Concurrent Bug Detection Method* proposes an improvement method for the maximum causal reduction algorithm used for concurrent bug detection, which uses directed graphs to filter and reduce the constraints generated during the detection process, so as to improve the speed of constraint solving and reduce the number of calls to the solver. Experiments have shown that this method reduces detection time by approximately 30% on benchmark cases.

Refinement-based Modeling and Formal Verification for Multiple Secure Partitions of TrustZone builds a refined TrustZone multi-security zone formal model, namely RMTEE, in the Isabelle/HOL theorem prover. The security enhancement mechanism for calling discretionary access control between partitions is designed for the hidden dangers of information flow security in the FF-A specification, finally verifying the refined relationship of the RMTEE model, the correctness of the event interface, and the security of information flow, and this indicates that the RMTEE model complies with confidentiality and integrity.

Coq Formalization of ZFC Set Theory for Teaching Scenarios builds a set theory proving environment easier to learn and use in the Coq theorem prover, which allows more textbook-style proofs through the support of forward reasoning mode and automatic proving strategy. The application of this tool in practical discrete mathematics teaching has achieved good results.

Consequence-based Axiom Pinpointing for Expressive Description Logic Ontologies proposes an axiomatic location method based on a successor decision algorithm for description logic ontology with strong expression ability and proves the correctness of the algorithm. Furthermore, it designs a reasoning tool for subsequent axiom positioning from the perspectives of white box and black box.

Shaowei Cai, Ph.D., professor, doctoral supervisor, presided over the National Excellent Youth Science Foundation project, has won Gold medals in SAT and SMT competitions, and won the Best Paper Award at the SAT 2021 Conference. In recent years, he has won awards in domestic and international EDA competitions. His research interests include constraint solving and combinatorial optimization.

Zhenbang Chen, Ph.D., professor, doctoral supervisor, presided over several National Natural Science Foundation projects, and won NASAC Young Software Innovation Award and ACM SIGSOFT Outstanding Paper Award. His research interests include program analysis, formal methods, and their applications.

Ji Wang, Ph.D., professor, doctoral supervisor. His research interest is highly trusted software.

Yongwang Zhao, Ph.D., Professor, School of Cyber Science and Technology, Zhejiang University, Director of Engineering Research Center of Mobile Security of Zhejiang Province. His research interests include formal logic and verification, operating system security, and programming language principles.

Bohua Zhan, Ph.D., associate professor, master's supervisor. His research interests include interactive theorem proving and modeling and verification of embedded systems.