Automata-Theoretical Decision Procedures For Path Feasibility of String Manipulating Programs

Zhilin Wu
Chinese Academy of Sciences

Time: 9:00 (Time in Beijing)
13:00 (Time in Auckland)
June 17, 2021 (Thursday)
Venue: Baixue Tang,UESTC Library

Abstract: The design and implementation of decision procedures for checking path feasibility in string-manipulating programs is an important problem, with such applications as symbolic execution of programs manipulating strings and automated detection of cross-site scripting (XSS) vulnerabilities in web applications. A (symbolic) path is given as a finite sequence of assignments and assertions (i.e. without loops), and checking its feasibility amounts to determining the existence of inputs that yield a successful execution. Modern programming languages (e.g.JavaScript, PHP, and Python) support many string operations, e.g. concatenation, replaceAll functions, string reverse, regular expressions (in a non-standard sense e.g. greedy/lazy Kleene star), string length, substring, indexof. Moreover, strings are also often implicitly modified during a computation in some intricate fashion, e.g. the user inputs in Web sites are usually preprocessed by HTML sanitizers, which can be naturally modeled as finite-state transducers. In this talk, I will present our recent work on automata-theoretical decision procedures for path feasibility of string manipulating programs. Our decision procedures deal with all the aforementioned complex and diverse string operations in a conceptually simple way, thus unifying and extending the existing decision procedures for string constraints. Moreover, we provide an efficient implementation of our decision procedures in a new string solver OSTRICH. We demonstrate the efficacy of OSTRICH against the state-of-the-art competitive solvers, e.g. CVC4 and Z3, by extensive experiments. This talk is based on our POPL 2018, POPL 2019, and ATVA 2020 publications.

Speaker Bio: Zhilin Wu is a research professor in State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences. He obtained his Phd. Degree from the same venue in 2007. His main research interests are program verification, automata theory, and computational logic. His research work appeared in international theoretical flagship conferences e.g. LICS, POPL, and CAV. He is the recipient of the 2020 CCF-IEEE CS Young Scientists Award.

Chengdu Algorithms and Logic Seminar is a series of online seminars organized by School of Computer Science and Engineering, University of Electronic Science and Technology of China, and School of Computer Science, University of Auckland that aims to promote collaborations in a broad range of topics in algorithms and logic.

Organizers: Bakhadyr Khoussainov, Jiamou Liu, and Mingyu Xiao
Email: myxiao@gmail.com (Mingyu Xiao)