Software Engineering Seminar (WiSe 2020/21)

Search Strategies in Concolic Testing

Description

Concolic testing (or dynamic symbolic execution) is an automatic test case generation technique that combines **conc**rete and symb**olic** execution of the system under test [1]. Symbolic execution employs program analysis to gather constraints on the execution path of the current concrete test input (the *path condition*). The obtained path condition can then be systematically negated and solved using a constraint solver in order to obtain new test inputs that exercise alternative paths. However, one of the main challenges of concolic testing is the *path explosion problem*, which makes an exhaustive exploration of the search space intractable. As a result, recent work has proposed advanced search strategies that aim to alleviate this problem, including techniques based on model checking [4] or pattern mining [2].

In this seminar, after examining the theoretic foundations of concolic testing and its traditional search strategies (e.g., DFS, BFS), the student is required to investigate and discuss recent advanced search strategies for concolic testing. The student should compare different approaches and give insights into future research.

References

[1] Roberto Baldoni, Emilio Coppa, Daniele Cono D'elia, Camil Demetrescu, and Irene Finocchi. A survey of symbolic execution techniques. *ACM Computing Surveys (CSUR)*, 51(3):1–39, 2018.

[2] Sooyoung Cha, Seonho Lee, and Hakjoo Oh. Template-guided concolic testing via online learning. In *2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 408–418. IEEE, 2018.

[3] Dongge Liu, Gidon Ernst, Toby Murray, and Benjamin IP Rubinstein. Legion: Best-first concolic testing. *arXiv preprint arXiv:2002.06311*, 2020.

[4] Xinyu Wang, Jun Sun, Zhenbang Chen, Peixin Zhang, Jingyi Wang, and Yun Lin. Towards optimal concolic testing. In *Proceedings of the 40th International Conference on Software Engineering*, pages 291–302, 2018.

Contacts

Hoang Lam Nguyen (`nguyehoa@informatik.hu-berlin.de`)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin