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 concrete and symbolic 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


Contacts

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