FuzzDiff: A Program Equivalence Checker based on feedback-directed fuzz testing and semantic analysis

Akash Purushottam Patil, Master of Science in Computer Science
University of Dublin, Trinity College, 2022

Supervisor: Prof. Vasileios Koutavas

Property-based fuzz testing with coverage guidance mechanism has proven to be very effective in finding bugs in high-level programs. This dissertation attempts to examine the possibility of proving functional equivalency of two Java programs using such feedback-directed fuzz testing techniques and semantic analysis, facilitated by a framework called JQF. An equivalence checker called FuzzDiff, in the form of a Maven project, is developed to compare the functional behaviour of two simple java programs having method with same signature and return type. JQF, which is based on JUnit QuickCheck, is used as the engine for generating feedback-directed random inputs being fed into these programs. A number of JUnit assertions determine the functional equivalence of the two input programs over the two stages. A Generic Generator class is also designed and implemented for generating random instances of custom Java objects. Moreover, the tool also applies additional tests for semantic analysis of the two input programs, where method invocations are traced and compared to comply with certain assertions. Finally, the tool is evaluated on a number of test programs in benchmarks used by tools like Hobbit and ARDiff, and the results are analyzed. Results show that FuzzDiff can effectively identify inequivalency but can be inconsistent in verifying equivalency of two Java programs. During evaluation, FuzzDiff also finds an incorrectly classified equivalent pair of program in ARDiff benchmark.