JOHANNES KEPLER
UNIVERSITÄT LINZ

o.Univ.-Prof. Dr.
Hanspeter Mössenböck
Institute for System Software

T +43 732 2468 4340
F +43 732 2468 4345
hanspeter.moessenboeck@jku.at

Secretary:
Karin Gusenbauer
Ext 4342
karin.gusenbauer@jku.at

Bachelor's Thesis

Feedback-directed fuzzing for the GraalVM compiler

Student:	Florian Schwarcz (k12105277)
Advisor:	Dr. Gergö Barany (Oracle Labs) Prof. Hanspeter Mössenböck
Begin:	01.03.2024

Fuzzing (also called randomized testing) is a software testing technique that submits large amounts of randomly generated inputs to a system under test. Fuzzing of compilers and other programming language implementations is very effective at finding bugs. Feedback-directed fuzzing takes information from the system under test and feeds it back to the fuzzer to guide its random input generation towards inputs that are considered particularly interesting. For example, code coverage information can guide the fuzzer towards new test cases that explore as yet uncovered program paths.

The GraalVM compiler is regularly fuzzed with a custom random Java source code generator. At the moment this generator does not use any notion of feedback. The goal of this project is to extend the code generator with feedback gathered from the GraalVM compiler's optimization log. The optimization log provides information on all optimizations performed by the compiler as it compiles a given input program. The extended generator will learn, either on-line or off-line, correspondences between Java language constructs and the GraalVM optimizations that they trigger. It will then use feedback from the optimization log to direct the selection of grammar rules during code generation. This will guide generation towards programs containing constructs that trigger less covered optimizations or combinations of optimizations.

The work's progress should be discussed with the advisor at least every 2 weeks. Please follow the guidelines of the Institute for System Software when preparing the written thesis. The deadline for submitting the written thesis is 30.09.2024.

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696