KLEE 实验课说明

一、 实验目的

KLEE 是 Stanford 的 Cristian Cadar 在 2008 年开发的基于符号执行的开源自动测试工具，该工具运行在 Linux 系统上，能够自动的对代码执行符号执行，进行覆盖测试和缺陷检测（例如除 0 错误，内存越界等问题）。

本实验的目的是：

1）熟悉 Linux 系统使用方式；

2）了解 LLVM 的架构和使用方式；

3）了解 Docker 使用或者 github 的使用方式；

4）了解并掌握基于约束的自动化测试工具的基本原理和使用。

二、实验内容

1. 利用 docker 镜像（http://klee.github.io/docker/ ）或者源代码编译（http://klee.github.io/build-llvm34/ ）的方式安装 KLEE；
2. 使用 KLEE 完成 tutorial 1 和 tutorial 2（http://klee.github.io/tutorials/ ），观察输出结果。
3. 查找或自己编写包含缺陷的程序（要求至少 50 行代码，且包含不少于 5 个缺陷），使用 KLEE 进行测试。

三、提交内容

1. 安装配置 docker（如果使用源代码编译，则忽略）和 KLEE 过程中遇到的问题和解决方式；
2. 运行完 tutorial 1 和 tutorial 2 之后得到的测试输出文件夹目录，例如

```
$ ls klee-last/
assembly.ll      run.istats       test000002.ktest
info             run.stats        test000003.ktest
messages.txt     test000001.ktest warnings.txt
```

目录路径中需要能够显示出个人的用户名；

3. 所使用的缺陷代码，以及提交 KLEE 检测后得到的错误文件内容。