jmtrace 实验报告

姓名：何伟　学号：171240537

文件结构

```
.
├── report.pdf
├── build.gradle
├── settings.gradle
└── src
    └── main
        └── java
            ├── ClassVisitorAdapter.java
            ├── MethodVisitorAdapter.java
            ├── PreMainAgent.java
            └── TraceInsn.java
```

运行

- 通过`gradle jar`获取依赖(asm库)，并打包生成`jmtrace-1.0-SNAPSHOT.jar`
- 使用`java -javaagent:./build/libs/jmtrace-1.0-SNAPSHOT.jar -jar something.jar`运行

实验过程

- 实验使用了`javaagent`捕获类的加载，再配合asm进行字节码插桩
- 通过检测对内存访问的指令，加入trace输出信息完成实验

实验困难

- 打包。由于gradle已经不在使用compile加载依赖，网上的教程较少，打包花了一些时间。
- asm。花了一些时间了解asm的用法。
- 对java字节码不熟悉。在构建函数调用的参数栈时，用到了DUP，DUP2等指令。由于对JAVA字节码不熟，没有注意到category1类型和category2类型的区别，导致对栈的修改发生错误，花了很长时间debug。