

PA2018.Spring.实验报告

实验人：贾聪

学号：141220045

时间：2018.5.21

2.1.1

使用 `hexdump` 命令查看测试用例的 `.img` 文件，所显示的 `.img` 文件的内容对应模拟内存的哪一个部分？指令在机器中表示的形式是什么？

对应虚拟内存地址从起始地址 `0x30000` 开始的数据。指令在机器中按照二进制形式编码，字节码对应相应的 `opcode`、`modrm` 等，从而完成指令含义的表达。二进制由机器的高低电平表示。

2.1.2

如果去掉 `instrexecute2op()` 函数前面的 `static` 关键字会发生什么情况？为什么？

如果去掉会发生链接错误。`static` 关键字使 `instr_execute_2op()` 成为本地符号，各个指令程序文件中均可声明。去掉后 `instr_execute_2op()` 成为全局函数并被编译为强符号，重复声明会发生链接错误。

2.1.3

为什么 `test-float` 会 `fail`？以后在写程序的时候要注意什么？

浮点数在加减后会有精度的损失（左规），导致结果并不是无限位数情况下的精确结果。在处理浮点数大小比较时，不能直接用等号比较，而应该在一个精度范围内进行比较运算，当结果在一定范围内就可以认为是近似相等的。比如 `c == 0.2` 可以改为 `c < 0.2 + 1e-5 || c > 0.2 - 1e-5`；

2.2

为什么在装载时要把内存中剩余的 `p_memsz - p_filesz` 字节的内容清零？

可能会残留先前加载的文件的字节，出现被定义但未被初始化的变量，统一初始化为0。

2.3

我们在 `add.c` 中定义了宏 `NR_DATA` , 同时也在 `add()` 函数中定义了局部变量 `c` 和形参 `a, b` , 但你会发现在符号表中找不到和它们对应的表项, 为什么会这样? 思考一下, 什么才算是一个符号(symbol)?

宏在编译过程中被取代变成了一段代码, 实际进行编译链接的是具体的代码段, 而宏不会被当作符号。同时局部变量, 形参都是用栈来处理, 不需要额外开辟空间来存储定位。符号应该有相应固定的地址, 并在符号表中定义。