实验报告



PA2-指令系统

学号 6319000359

姓名 张明君

|  |
| --- |
| 实验进度（任务自查表） |
| |  |  | | --- | --- | | 序号 | 是否已完成 | | 必做任务 1 | 是 | | 必做任务 2 | 是 | | 必做任务 3 | 是 | | 必做任务 4 | 是 | | 必做任务 5 | 是 | | 选做任务 1 | 是 | | 选做任务 2 | 否 |   **必做任务1：运行用户程序 mov-c**  **必做任务2：实现更多指令**  **必做任务3：实现 binary scaling**  **必做任务4：为表达式求值添加变量的支持**  **选做任务1: 打印栈帧链**  **必做任务5：实现 loader**  **选做任务：知己知彼**  **选做任务 :偷龙转凤**  **选做任务：头龙转凤** |
| 思考题（请注明题号，如思考题1，思考题2，. . .） |
| **思考题 1：main 函数返回到哪里**  查看 testcase 的相关代码,你知道用户程序从 main 函数返回之后会跳转到哪 里吗？如果用户程序在 GNU/Linux 中运行, 问题的答案又是什么？  **答案：**当把.c 文件运行之后 我们可以查看log.txt, 而且函数nemu\_trap()是来判断运行的觉果是不是正确，它会停在Nemu 程序中，那么它会跳转到nemu的main()中及等用户继续输入操作指令。  **思考题 2：比较 FLOAT 和 float**  FLOAT 和 float 类型的数据都是 32 位, 它们都可以表示 2^32 个不同的数, 但由 于表示方法不一样, FLOAT 和 float 能表示的数集是不一样的。思考一下, 我们 用 FLOAT 来模拟表示 float, 这其中隐含着哪些取舍?  **答案：**FLOAT 类型的加法可以直接用整数 加法来进行。使用**FLOAT**类型来模拟实数运算比较方便。除了乘除法 需要额外实现之外，其余运算都可以直接使用相应的整数运算来进行。  **思考题 3：消失的符号**  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)？  **答案：**符号表是一种存储代码中的变量函数调用等的数据库。符号表以key-value 来存储数据。当解析器读取源代码，遇到声明部分时，便给符号表添加一条记录，如果变量或函数脱离了它的作用范围时，便将它们对应的记录从表中删除。所以函数内的局部参数在出作用域范围后会在符号表中被删除，而形参没有直接具体的数据存储意义，不在符号表中存储。  **思考题 4：堆和栈在哪里?**  我们提到了代码和数据都在可执行文件里面, 但却没有提到堆(heap)和栈 (stack)。为什么堆和栈的内容没有放入可执行文件里面？那程序运行时刻用到 的堆和栈又是怎么来的?  **答案：**因为堆和栈中数据的变化比较频繁，如果放进可执行文件中读取速度会变慢。所以当程序运行的时候，从内部里面来申请栈和堆的使用，加快运行速度。  **思考题 5：如何识别不同格式的可执行文件？**  如果你在 GNU/Linux 下执行一个从 Windows 拷过来的可执行文件, 将会报告" 格式错误"。思考一下, GNU/Linux 是如何知道"格式错误"的？  **答案：**ELF和PE文件整体结构并无大区别，都有存储文件信息的head，data等且PE文件头也定义了段数，符号表位置等信息，但是ELF文件头还有魔数一值，linux每次读取elf头文件的时候，都会确认魔数是否正确，以防读入的不是elf文件，因此可以来判断文件格式，如果不是即可确认“格式错误”。  **思考题 6：冗余的属性？**  使用 readelf 查看一个 ELF 文件的信息, 你会看到一个 segment 包含两个大小 的属性, 分别是 FileSiz 和 MemSiz, 这是为什么? 再仔细观察一下, 你会发现 FileSiz 通常不会大于相应的 MemSiz, 这又是为什么?  **答案：**FileSize和memSize分别表示程序头在文件中和在内存中的大小。 |
| 实验遇到的问题、思考、解决办法（可以不填写） |
|  |
| 实验心得（可以不填写） |
|  |