《计算机系统基础实验》任务书

# **实验二 汇编语言编程基础**

**一．实验目的和要求**

1. 掌握汇编源程序编辑工具、汇编程序、连接程序、调试工具的使用；
2. 熟悉分支、循环程序、子程序的结构，掌握分支、循环、子程序的调试方法；
3. 加深对转移指令、子程序调用和返回指令及一些常用的汇编指令的理解。

**二．实验内容**

（上机实验环境说明：建议使用Linux32位编程环境（建议使用Linux虚拟机）。源程序编辑工具可以使用vi（或使用windows下的vscode、记事本等编辑器，然后共享到虚拟机中）；汇编程序使用as;连接程序使用ld；（或使用gcc进行编译和链接）；调试工具使用gdb。具体介绍可参见《linux的汇编语言程序设计》第4章。

任务2.1 习题三，第2题。

要求：（1）分别记录执行到“mov $10, %ecx”和“mov $1, %eax”之前的EBX,EBP,ESI,EDI各是多少。

（2）记录程序执行到退出之前数据段开始40个字节的内容，指出 程序运行结果是否与设想的一致。

(3)在标号lopa前加上一段程序，实现新的功能：先显示提示信息“Press any key to begin!”, 然后，在按了一个键之后继续执行lopa处的程序。

**操作提示：**假设汇编语言程序名为ex1.s,可使用命令：gcc -g -no-pie ex1.s -o ex1(第一条指令地址为main的汇编语言程序)字节生成可执行程序。

as -g -32 -o ex1.o ex1.s编译生成.o文件(第一条指令地址为\_start的汇编语言程序)，然后用ld命令链接：ld -m elf\_i386 -o ex1 ex1.o

可使用gdb调试，先单步执行各个语句，每执行一条语句，都应观察数据段中的内容以及相应寄存器的变化。其次，单步执行循环体两遍且正确理解了循环体语句的含义后，可在“mov $1, %eax”处设置断点，然后直接执行到断点处，回答(1)和(2)的问题。

任务2.2 习题三，第3题。

要求：(1) 内存单元中数据的访问采用变址寻址方式。

(2) 记录程序执行到退出之前数据段开始40个字节的内容，检查 程序运行结果是否与设想的一致。

(3) 观察并记录机器指令代码在内存中的存放形式，并与反汇编语句及自己编写的源程序语句进行对照，也与任务2做对比。（相似语句记录一条即可，重点理解机器码与汇编语句的对应关系，尤其注意操作数寻址方式的形式）。

任务2.3 **设计实现一个数据处理的程序**

有一个计算机系统运行状态的监测系统会按照要求收集三个状态信息a，b，c（均为有符号双字整型数）。假设4组状态信息已保存在内存中。对每组的三个数据进行处理的模型是f=(5a+b-c+100)/128（最后结果只保留整数部分）。当f<100时，就将该组数据复制到LOWF存储区，当f=100时，就将该组数据复制到MIDF存储区，当f>100时，就将该组数据复制到HIGHF存储区。

每组数据的定义方法可以参考如下：

sdmid .fill 9, 1, 0 # 每组数据的流水号（可以从1开始编号）

sda .long 256809 # 状态信息a

sdb .long -1023 # 状态信息b

sdc .long 1265 # 状态信息c

sf .long 0 # 处理结果f

请编写完整的汇编语言程序，并按照要求设计子程序。

(1) 编写一子程序calculate，完成f的计算并保存，并且子程序的入口参数为esi（调用子程序前后esi的值不变），保存状态信息a的地址，若f=100，则(eax)=0, f>100, 则(eax)=1, 若f<100则(eax)=-1，返回eax；先按照不考虑溢出的要求编写程序，再按照考虑溢出的要求修改程序；

(2) 编写一子程序copy\_data，要求用堆栈传递参数，实现一组存储区状态信息的复制，要求每次拷贝4字节，多余的1个字节单独拷贝，参数为待复制的存储区的首地址和拷贝的目标地址，拷贝的字节长度。

(3) 查看运行到返回操作系统的指令之前，三个存储区域LOWF、MIDF、HIGHF内前50字节的值，只需要截图即可。

(4) 熟悉加减乘除等运算指令，内存拷贝方法。思考：如果三个状态信息是无符号数，程序需要做什么调整？

可参考的程序框架

.section .data

sdmid: .ascii "000111", "\0\0\0" # 每组数据的流水号（可以从1开始编号）

sda: .long 512 # 状态信息a

sdb: .long -1023 # 状态信息b

sdc: .long 1265 # 状态信息c

sf: .long 0 # 处理结果f

.ascii "000222","\0\0\0"

.long 256809 # 状态信息a

.long -1023 # 状态信息b

.long 2780 # 状态信息c

.long 0 # 处理结果f

.ascii "000333","\0\0\0"

.long 2513# 状态信息a

.long 1265 # 状态信息b

.long 1023 # 状态信息c

.long 0 # 处理结果f

.ascii "000444","\0\0\0"

.long 512 # 状态信息a

.long -1023 # 状态信息b

.long 1265 # 状态信息c

.long 0 # 处理结果f

.ascii "555555","\0\0\0"

.long 2513

.long 1265

.long 1023

.long 0

.ascii "666666","\0\0\0"

.long 256800

.long -2000

.long 1000

.long 0

num = 6

midf: .fill 9, 1, 0

.long 0, 0, 0, 0

.fill 9, 1, 0

.long 0,0,0,0

.fill 9, 1,0

.long 0,0,0,0

highf: .fill 9, 1, 0

.long 0, 0, 0, 0

.fill 9, 1, 0

.long 0,0,0,0

.fill 9,1,0

.long 0,0,0,0

lowf: .fill 9, 1, 0

.long 0, 0, 0, 0

.fill 9, 1, 0

.long 0,0,0,0

.fill 9,1,0

.long 0,0,0,0

len=25

.section .text

.global \_start

\_start:

……

mov $1, %eax

mov $0, %ebx

int $0x80

.type calculate @function

calculate:

……

ret

.type copy\_data @function

copy\_data:

……

ret

***--------------实验内容描述完毕。以下是相关说明，请认真阅读------------***

* 进度提示：

实验二课内学时4，即占用一周课内实验课时。

* 自行设定需要探究学习的问题提示：

如何设定需要探究的问题？途径一,改变（包括增加、减少、修改等）已有的实现方法、语句、数据定义等，观察是否会有意想不到的效果；途径二，把自己平时未搞清楚的问题纳入到实验中，通过实验来帮助理解；途径三，自行设置新的问题并通过实验观察来解决。

（这些问题及结果可按照合适的方式纳入到自己写的实验报告中）