## 实验三、数据分支控制实验

1. 实验目的

了解数据分支流程。

识别汇编码中的分支跳转条件。并了解如何修改分支条件。

二、实验内容

1、下面是do\_loop函数的定义，请自己编写一个main函数，要求如下：

1)在main函数中调用do\_loop

2)main函数能从stdin中接收输入参数并传递给do\_loop

3)使用命令gcc -O1 -ggdb do\_loop.c -o do\_loop得到可执行程序do\_loop

short do\_loop(short x, short y, short k) {

do {

x\*=(y%k) ;

k--;

} while ((k>0) && (y>k));

return x;

}

实验内容如下：

1. 输入参数x=2, y = 4000, k=3使用gdb进入do\_loop的第一次循环：

a在执行指令cltd前%edx的值是多少？

b在刚执行完cltd后%edx的值是多少？

c请回答为cltd指令的作用

d在执行指令%idiv后%edx的值又变为了多少？请解释这种变化。

（2）使用输入x=2，y=40000，k=3重复（1）的内容

Hints:

1. 使用gdb do\_loop进入gdb
2. 使用break do\_loop设置breakpoint
3. run
4. 使用Ctrl-x Ctrl-a组合键进入TUI模式
5. layout asm
6. si
7. 查看寄存器edx的值print $edx

8.查看do\_loop汇编码disassemble do\_loop

如果TUI模式有问题请直接时候用gdb查看内存及寄存器的值。

2、（简单）给定if\_else.s文件，完成如下要求：

修改if\_else.s中if\_else片段，只允许修改分支条件，不需修改分支中的内容，达到如下要求。

A：输入 12 15 ，要求现在if\_else的返回值为1 （原来返回值为0）

B：输入学号后四位，（如学号后四位是1234则输入12 34 ）要求输出结果为2

（A、B分别得到不同的if\_else.s文件，分别重新命名为if\_else\_A.s以及if\_else\_B.s）

Hints：

a：可以使用gcc if\_else.s –o if\_else将.s文件生成可执行程序。可执行程序中会根据输入将结果输出到屏幕。（可具此判断修改后的.s文件是否达到要求）

b：if\_else片段如下：可修改语句已用红色标出

if\_else:

.LFB0:

.cfi\_startproc

pushl %ebp

.cfi\_def\_cfa\_offset 8

.cfi\_offset 5, -8

movl %esp, %ebp

.cfi\_def\_cfa\_register 5

subl $16, %esp

cmpl $0, 8(%ebp)

jle .L2

cmpl $29, 12(%ebp)

jg .L2

movl $0, -4(%ebp)

jmp .L3

.L2:

cmpl $0, 8(%ebp)

jle .L4

cmpl $30, 12(%ebp)

jle .L4

movl $1, -4(%ebp)

jmp .L3

.L4:

movl $2, -4(%ebp)

.L3:

movl -4(%ebp), %eax

leave

.cfi\_restore 5

.cfi\_def\_cfa 4, 4

ret

.cfi\_endproc

.LFE0:

.size if\_else, .-if\_else

.section .rodata

.LC0:

.string "%d %d"

.LC1:

.string "%d\n"

.text

.globl main

.type main, @function

1. 给定一个可执行程序switch，并根据汇编码完成如下要求：
2. 利用gdb，分别输入参数：

A: x = 2；

B: x = 6；

C: x = 9；

D: x = 3;

观察每个输入后switch\_case函数的返回值各是多少？

2）输入学号最后一位，观察switch\_case函数的返回值。

3）将如下函数填充完整：

int switch\_case(int x){

int result =0;

switch(x){

case \_\_:

result = x\*\_\_;

break;

case \_\_:

result = x\*\_\_;

break;

case \_\_:

result = x\*\_\_;

break;

default:

result = \_\_;

}

return result += \_\_;

}

使用命令objdump –d switch > switch\_case.s得到的函数switch\_case的汇编代码。并将源码填充完整。

Hints:

1.可以使用gdb运行观察每个寄存器的值，参考实验一的提示。

**实验报告要求：**

请提交一个压缩包151220000.zip到ftp的lab03文件夹（注意修改学号和压缩格式，如果需要覆盖第一次提交，请提交151220000\_1.zip，依次类推）。压缩包内部应该是一个目录。

151220000.zip解压后获得目录内容如下：

151220000

|----if\_else\_A.s

|----if\_else\_B.s

|----report.pdf（包含三个实验内容的结果，细节可截图说明）