

Homework 5

1. Indicate the status (0, 1 or – to indicate unaffected) of the following flag registers after the instructions being executed. Assume 5 in %eax and -7 in %ebx. The following instructions execute independently and would **NOT** affect each other.

Ins	CF	ZF	SF	OF
leal (%edx,%edx,2),%edx	-	-	-	-
addl %eax, %ebx	0	0	1	0
xorl %eax, %eax	0	0	0	0
cmpl %ebx, %eax	0	0	0	0

2. Translate the following assembly into C codes. Note that you can name local variables represented by 28(%esp), 24(%esp)... freely as you like.

```
    movl $1, 28(%esp)
    movl $1, 24(%esp)
    movl $10, 16(%esp)
    movl $3, 20(%esp)
    jmp  L2
L3:
    movl 28(%esp), %eax
    movl %eax, 12(%esp)
    movl 24(%esp), %eax
    movl %eax, 28(%esp)
    movl 12(%esp), %eax
    addl %eax, 24(%esp)
    incl    20(%esp)
L2:
    cmpl $10, 20(%esp)
    jle  L3
    (Following code omitted...)
```

计算第 10 个斐波那契数。

```
int a = 1;
int b = 1;
int n = 10;
int i;
for (i = 3; i <= 10; ++i) {
    int temp = a;
    a = b;
    b += temp;
}
```

3. Translate the following switch statements into assembly using jump table.

```

int x = <some value>;
int result = 0;
switch (x) {
    case 64:
        result = x + x;
        break;
    case 66:
        result = x + 10;
        break;
    case 68:
        result = x * 2;
        // Notice: there is no break here!
    case 69:
        result = result + 1;
        break;
    default:
        result = 3;
        break;
}

```

Jump Table 部分: 标签名称不唯一，但必须与后面的代码一一对应。

```

.section .rdata,"dr"
.align 4
L9:
    .long    L3
    .long    L2
    .long    L4
    .long    L2
    .long    L5
    .long    L6

```

代码部分: [x]与[result]可以被替换成 x(%esp)形式或者某些可用的寄存器，只要能够代表这两个变量即可，形式不重要。

```

.text
L3:
    movl    [x], %eax
    addl    %eax, %eax
    movl    %eax, [result]
    jmp     L11
L4:
    movl    [x], %eax
    addl    $10, %eax
    movl    %eax, [result]
    jmp     L11
L5:
    movl    [x], %eax
    sall    %eax
    movl    %eax, [result]
L6:
    incl    [result]
    jmp     L11
L2:
    movl    $3, [result]
    nop
    jmp     L11
L11:
    <the following codes omitted...>

```

4. Draw a stack for each step when the following function is being called and indicate where %ebp and %esp points. Here is an example where the first step takes place.
 int foo(int a, int b, int c);



