| 得分 |
|---|
| |

**第四题（10 分）**

一个函数如下，其中部分代码被隐去，请通过gdb调试信息补全代码（4分）。

```
int f(int n, int m) {
    if (m > 0) {
        if (______________) {
            int r = ________________________;
            return ________________________;
        }
        else if (__________________) {
            return 1;
        }
    }
    return 0;
}
```

如下是通过"gcc -g -O2"命令编译后，在gdb中通过"disas f"命令得到的反汇编代码，其中有两个汇编指令不全，请补全这两条汇编指令（2分）。

```
0x00000000004004e0 <f+0>:      mov    %rbx,-0x10(%rsp)
0x00000000004004e5 <f+5>:      mov    ________________________
0x00000000004004ea <f+10>:     xor    %eax,%eax
0x00000000004004ec <f+12>:     sub    $0x10,%rsp
0x00000000004004f0 <f+16>:     test   %esi,%esi
0x00000000004004f2 <f+18>:     mov    %edi,%ebp
0x00000000004004f4 <f+20>:     mov    %esi,%ebx
0x00000000004004f6 <f+22>:     jle    0x400513 <f+51>
0x00000000004004f8 <f+24>:     cmp    $0x1,%edi
0x00000000004004fb <f+27>:     jle    0x400521 <f+65>
0x00000000004004fd <f+29>:     lea    -0x1(%rbp),%edi
0x0000000000400500 <f+32>:     callq  0x4004e0 <f>
0x0000000000400505 <f+37>:     lea    -0x1(%rax,%rbx,1),%edx
0x0000000000400509 <f+41>:     mov    %edx,%eax
0x000000000040050b <f+43>:     sar    $0x1f,%edx
0x000000000040050e <f+46>:     idiv   %ebp
0x0000000000400510 <f+48>:     lea    0x1(%rdx),%eax
```

```
0x0000000000400513 <f+51>:     mov    ________________
0x0000000000400517 <f+55>:     mov    0x8(%rsp),%rbp
0x000000000040051c <f+60>:     add    $0x10,%rsp
0x0000000000400520 <f+64>:     retq
0x0000000000400521 <f+65>:     sete   %al
0x0000000000400524 <f+68>:     movzbl %al,%eax
0x0000000000400527 <f+71>:     jmp    0x400513 <f+51>
```

已知在调用函数f(4, 3)时，我们在函数f中指令retq处设置了断点，下面列出的是程序在第一次运行到断点处暂停时时，相关通用寄存器的值。请根据你对函数及其汇编代码的理解，填写当前栈中的内容。如果某些内存位置处内容不确定，请填写X。（4分）

| | |
|---|---|
| rax | 0x1 |
| rbx | 0x3 |
| rcx | 0x3 |
| rdx | 0x309c552970 |
| rsi | 0x3 |
| rdi | 0x1 |
| rbp | 0x2 |
| rsp | 0x7fffffffe340 |
| rip | 0x400520 |

| | |
|---|---|
| 0x7fffffffe38c | |
| 0x7fffffffe388 | |
| 0x7fffffffe384 | |
| 0x7fffffffe380 | |
| 0x7fffffffe37c | |
| 0x7fffffffe378 | |
| 0x7fffffffe374 | |
| 0x7fffffffe370 | |
| 0x7fffffffe36c | |
| 0x7fffffffe368 | |
| 0x7fffffffe364 | |
| 0x7fffffffe360 | |
| 0x7fffffffe35c | |
| 0x7fffffffe358 | |
| 0x7fffffffe354 | |
| 0x7fffffffe350 | |
| 0x7fffffffe34c | |
| 0x7fffffffe348 | |
| 0x7fffffffe344 | |
| 0x7fffffffe340 | |
| 0x7fffffffe33c | |
| 0x7fffffffe338 | |
| 0x7fffffffe334 | |
| 0x7fffffffe330 | |
| 0x7fffffffe32c | |
| 0x7fffffffe328 | |
| 0x7fffffffe324 | |
| 0x7fffffffe320 | |