Princeton University
COS 217: Introduction to Programming Systems
Assembler Output for powerfunction via gdb

```
$ gcc –c powerfunction.s

$ gdb powerfunction.o

(gdb) x/17i power
0x0 <power>:    push   %ebp
0x1 <power+1>:  mov    %esp,%ebp
0x3 <power+3>:  push   $0x1
0x5 <power+5>:  push   $0x0
0x7 <power+7>:  movl   $0x1,0xfffffff8(%ebp)
0xe <loop1>:    mov    0xfffffff8(%ebp),%eax
0x11 <loop1+3>: cmp    0xc(%ebp),%eax
0x14 <pcPrompt2+2>:     jg     0x24 <loopend1>
0x16 <pcPrompt2+4>:     mov    0xfffffffc(%ebp),%eax
0x19 <pcPrompt2+7>:     imull  0x8(%ebp)
0x1c <pcPrompt2+10>:    mov    %eax,0xfffffffc(%ebp)
0x1f <pcPrompt2+13>:    incl   0xfffffff8(%ebp)
0x22 <pcPrompt2+16>:    jmp    0xe <loop1>
0x24 <loopend1>:        mov    0xfffffffc(%ebp),%eax
0x27 <loopend1+3>:      mov    %ebp,%esp
0x29 <pcScanfFormat+1>: pop    %ebp
0x2a <pcScanfFormat+2>: ret

(gdb) x/43b power
0x0 <power>:    0x55    0x89    0xe5    0x6a    0x01    0x6a    0x00    0xc7
0x8 <power+8>:  0x45    0xf8    0x01    0x00    0x00    0x00    0x8b    0x45
0x10 <loop1+2>: 0xf8    0x3b    0x45    0x0c    0x7f    0x0e    0x8b    0x45
0x18 <pcPrompt2+6>:     0xfc    0xf7    0x6d    0x08    0x89    0x45    0xfc    0xff
0x20 <pcPrompt2+14>:    0x45    0xf8    0xeb    0xea    0x8b    0x45    0xfc    0x89
0x28 <pcScanfFormat>:   0xec    0x5d    0xc3
```

Translation of movl $1, -8(%ebp)

```
11000111 01000101 11111000 00000001 00000000 00000000 00000000
This is a movl instruction whose first operand is immediate
         The second operand is a memory operand of the form onebytedisplacement(%ebp)
                  The displacement in the memory operand is -8
                           The immediate operand is 1
```

```
(gdb) x/36i main
0x2b <pcResult>:        push   %ebp
0x2c <pcResult+1>:      mov    %esp,%ebp
0x2e <pcResult+3>:      push   $0x0
0x30 <pcResult+5>:      push   $0x0
0x32 <pcResult+7>:      push   $0x0
0x34 <pcResult+9>:      push   $0x0
0x39 <pcResult+14>:     call   0x3a <pcResult+15>
0x3e <pcResult+19>:     add    $0x4,%esp
0x41 <pcResult+22>:     lea    0xfffffffc(%ebp),%eax
0x44 <pcResult+25>:     push   %eax
0x45 <pcResult+26>:     push   $0x28
0x4a <pcResult+31>:     call   0x4b <pcResult+32>
0x4f <pcResult+36>:     add    $0x8,%esp
0x52 <pcResult+39>:     push   $0x12
0x57 <pcResult+44>:     call   0x58 <pcResult+45>
0x5c <pcResult+49>:     add    $0x4,%esp
0x5f <pcResult+52>:     lea    0xfffffff8(%ebp),%eax
0x62 <pcResult+55>:     push   %eax
0x63 <pcResult+56>:     push   $0x28
0x68 <pcResult+61>:     call   0x69 <pcResult+62>
0x6d <pcResult+66>:     add    $0x8,%esp
0x70 <pcResult+69>:     pushl  0xfffffff8(%ebp)
0x73 <pcResult+72>:     pushl  0xfffffffc(%ebp)
0x76 <pcResult+75>:     call   0x0 <power>
0x7b <pcResult+80>:     add    $0x8,%esp
0x7e <pcResult+83>:     mov    %eax,0xfffffff4(%ebp)
0x81 <pcResult+86>:     pushl  0xfffffff4(%ebp)
0x84 <pcResult+89>:     pushl  0xfffffff8(%ebp)
0x87 <pcResult+92>:     pushl  0xfffffffc(%ebp)
0x8a <pcResult+95>:     push   $0x2b
0x8f <pcResult+100>:    call   0x90 <pcResult+101>
0x94 <pcResult+105>:    add    $0x10,%esp
0x97 <pcResult+108>:    mov    $0x0,%eax
0x9c <pcResult+113>:    mov    %ebp,%esp
0x9e <pcResult+115>:    pop    %ebp
0x9f <pcResult+116>:    ret

(gdb) x/117b main
0x2b <pcResult>:        0x55    0x89    0xe5    0x6a    0x00    0x6a    0x00    0x6a
0x33 <pcResult+8>:      0x00    0x68    0x00    0x00    0x00    0x00    0xe8    0xfc
0x3b <pcResult+16>:     0xff    0xff    0xff    0x83    0xc4    0x04    0x8d    0x45
0x43 <pcResult+24>:     0xfc    0x50    0x68    0x28    0x00    0x00    0x00    0xe8
0x4b <pcResult+32>:     0xfc    0xff    0xff    0xff    0x83    0xc4    0x08    0x68
0x53 <pcResult+40>:     0x12    0x00    0x00    0x00    0xe8    0xfc    0xff    0xff
0x5b <pcResult+48>:     0xff    0x83    0xc4    0x04    0x8d    0x45    0xf8    0x50
0x63 <pcResult+56>:     0x68    0x28    0x00    0x00    0x00    0xe8    0xfc    0xff
0x6b <pcResult+64>:     0xff    0xff    0x83    0xc4    0x08    0xff    0x75    0xf8
0x73 <pcResult+72>:     0xff    0x75    0xfc    0xe8    0x85    0xff    0xff    0xff
0x7b <pcResult+80>:     0x83    0xc4    0x08    0x89    0x45    0xf4    0xff    0x75
0x83 <pcResult+88>:     0xf4    0xff    0x75    0xf8    0xff    0x75    0xfc    0x68
0x8b <pcResult+96>:     0x2b    0x00    0x00    0x00    0xe8    0xfc    0xff    0xff
0x93 <pcResult+104>:    0xff    0x83    0xc4    0x10    0xb8    0x00    0x00    0x00
0x9b <pcResult+112>:    0x00    0x89    0xec    0x5d    0xc3

(gdb) quit
```