

## 7 Машин програм III: Процедур

1. Дотроо a0-a8 хүртэл дотоод утгууд агуулсан P функцийг авч үзье. Уг функц Q функцэд тэдгээр дотоод хувьсагчдыг параметрээр дамжуулсан. P функцийн эхний ассемблер кодыг хэсэг:

P:

```
pushq %r15
pushq %r14
pushq %r13
pushq %r12
pushq %rbp
pushq %rbx
subq $24, %rsp
movq %rdi, %rbx
leaq 1(%rdi), %r15
leaq 2(%rdi), %r14
leaq 3(%rdi), %r13
leaq 4(%rdi), %r12
leaq 5(%rdi), %rbp
leaq 6(%rdi), %rax
movq %rax, (%rsp)
leaq 7(%rdi), %rdx
movq %rdx, 8(%rsp)
movl $0, %eax
call Q
```

- (a) Дуудах талд хадгалагдах регистрт (“callee-saved”) хадгалагдсан дотоод утгууд аль нь вэ?
- (b) Стак дээр хадгалагдсан дотоод утгууд аль нь вэ?
- (c) Програм яагаад бүх дотоод утгуудыг дуудах талд хадгалагдах регистрт (“callee-saved”) оноож чадахгүй байгааг тайлбарла.

2. Дараах бүтэцтэй Си функц өгөгдсөн.

```
long rfun(unsigned long x) {
    if (-----) {
        return -----;
    unsigned long nx = -----;
    long rv = rfun(nx);
    return -----;
}
```

Тэгвэл GCC дараах ассемблер кодыг үүсгэсэн.

**rfun:**

```
pushq %rbx
movq %rdi, %rbx
movl $0, %eax
testq %rdi, %rdi
je .L2
shrq $2, %rdi
call rfun
addq %rbx, %rax
.L2:
popq %rbx
ret
```

- (a) Дуудах талд хадгалагдах регистр болох `%rbx`-т *rfun* функц ямар утга хадгалж байгааг ол.
- (b) Дээрх Си кодыг нөхөж бич.