7 Машин програм III: Procedures

1. Дараах машин код өгөгдсөн.

```
    Disassembly of last(long u, long v)
    u in %rdi, v in %rsi
1   0000000000400540 <last>:
2     400540:  48 89 f8              mov    %rdi,%rax        L1: u
3     400543:  48 0f af c6           imul   %rsi,%rax        L2: u*v
4     400547:  c3                    retq                    L3: Return

    Disassembly of last(long x)
    x in %rdi
5   0000000000400548 <first>:
6     400548:  48 8d 77 01           lea    0x1(%rdi),%rsi   F1: x+1
7     40054c:  48 83 ef 01           sub    $0x1,%rdi        F2: x-1
8     400550:  e8 eb ff ff ff        callq  400540 <last>    F3: Call last(x-1,x+1)
9     400555:  f3 c3                 repz retq               F4: Return
        .
        .
        .
10    400560:  e8 e3 ff ff ff        callq  400548 <first>   M1: Call first(10)
11    400565:  48 89 c2              mov    %rax,%rdx        M2: Resume
```

Тэгвэл анх *first(10)* гэж функц дуудагдахаас эхлэн дуусах хүртэл программын алхам бүрийг дараах хүснэгтэд нөх. Баруун талд байгаа цэнхрээр бичигдсэн лабелийн дагуу нөхөхийг анхаарна уу.

Instruction			State values (at beginning)					
Label	PC	Instruction	%rdi	%rsi	%rax	%rsp	*%rsp	Description
M1	0x400560	callq	10	—	—	0x7fffffffe820	—	Call first(10)
F1								
F2								
F3								
L1								
L2								
L3								
F4								
M2								

2. *procprob* функц нь *u, a, v, b* гэсэн 4 ширхэг аргументтай. Эдгээр аргументууд нь нэг бол тэмдэгтэй бүхэл тоо эсвэл тэмдэгтэй бүхэл тоог заах заагч. Эдгээр тоонууд нь өөр өөр

хэмжээтэй. Функцийн доторх нь дараах хэлбэртэй.

```
*u += a;
*v += b;
return sizeof(a) + sizeof(b);
```

Уг кодыг хөрвүүлэхэд дараах машин код гарч ирсэн.

```
procprob:
  movslq %edi, %rdi
  addq   %rdi, (%rdx)
  addb   %sil, (%rcx)
  movl   $6, %eax
  ret
```

Тэгвэл параметрүүд нь ямар дараалалтай ямар төрлийнх байсныг ол. Хоёр зөв хариу байх боломжтой. Хариу бүрийг бич.

Дараагийн хуудсанд үргэлжлэл бий.

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 ассембер 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.