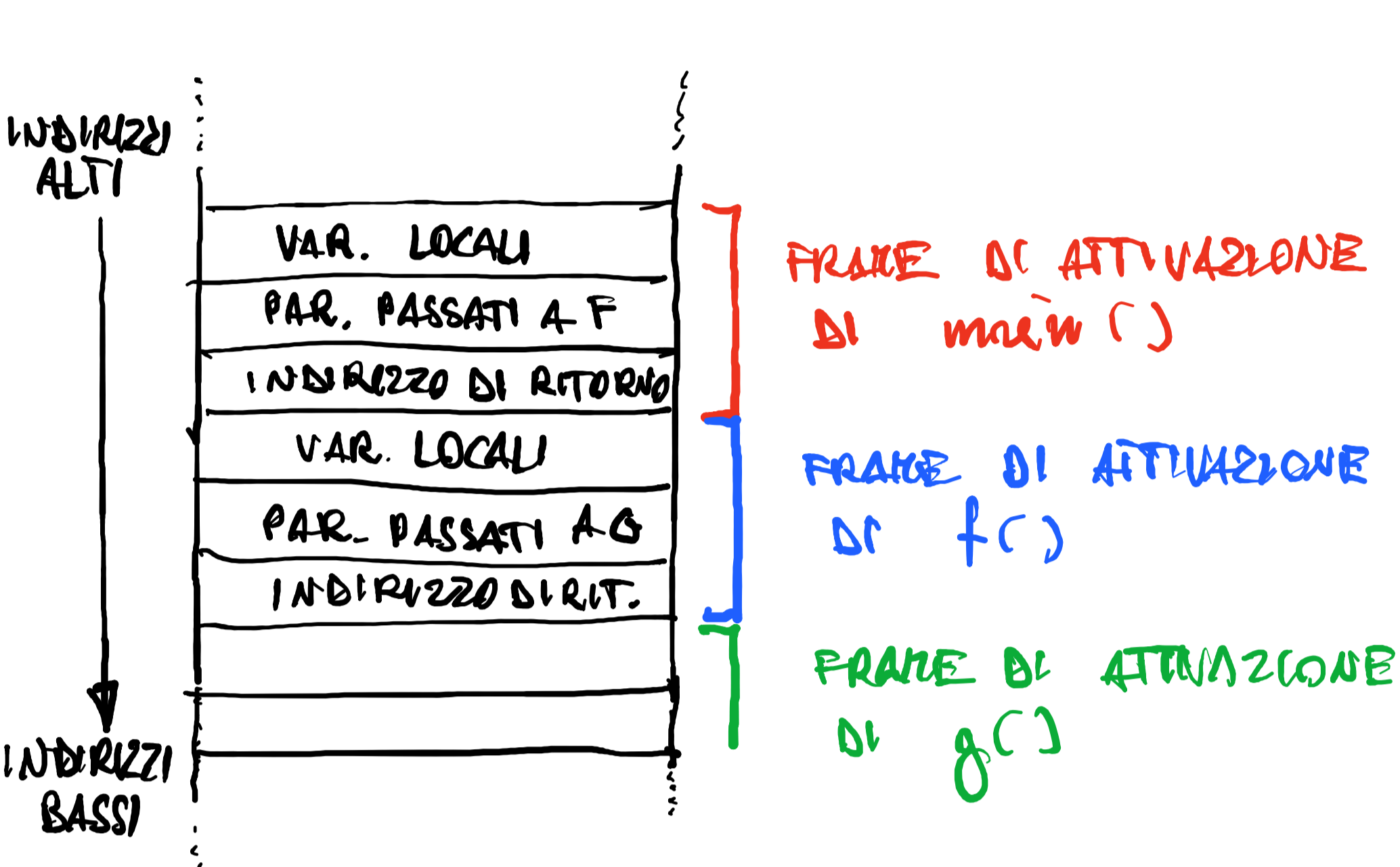
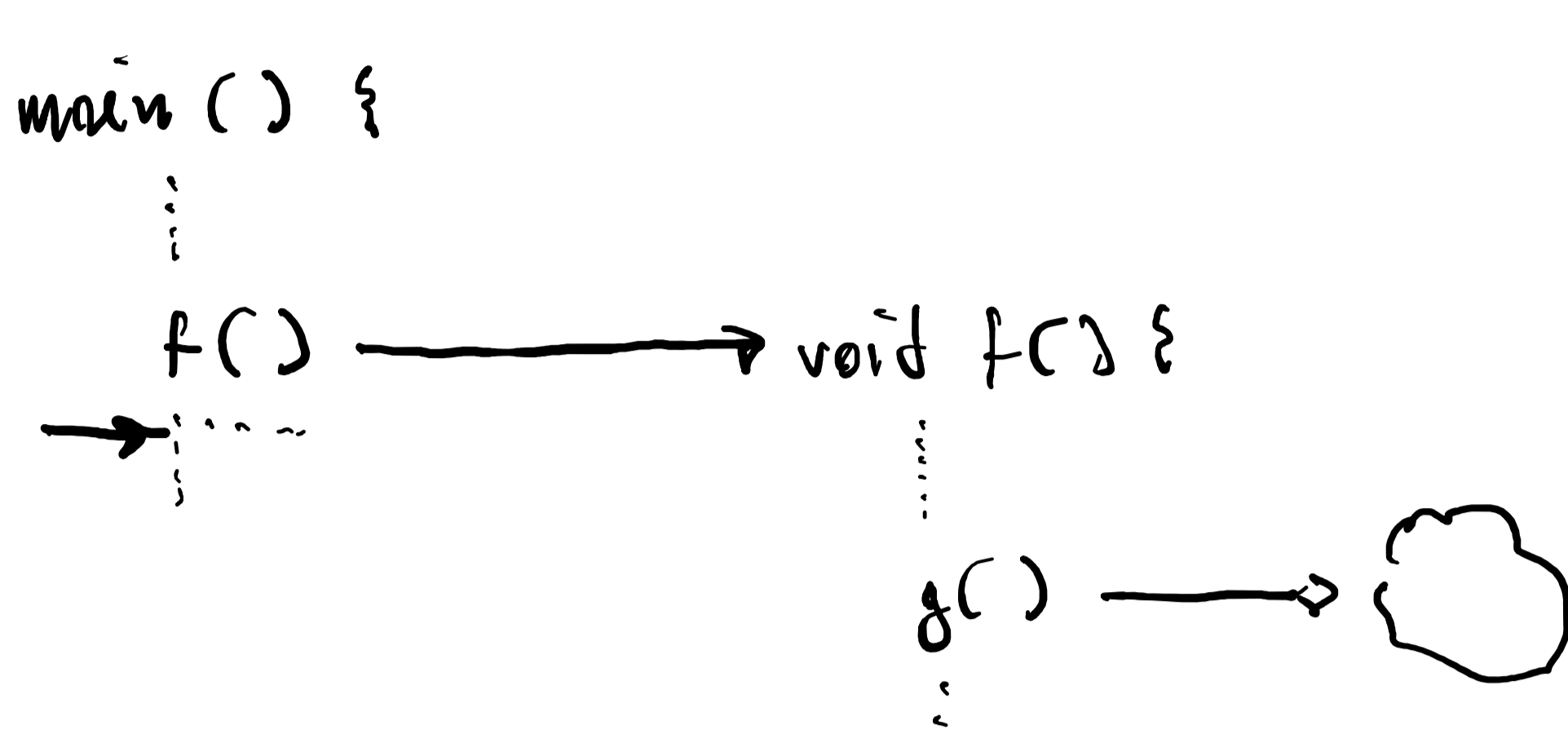
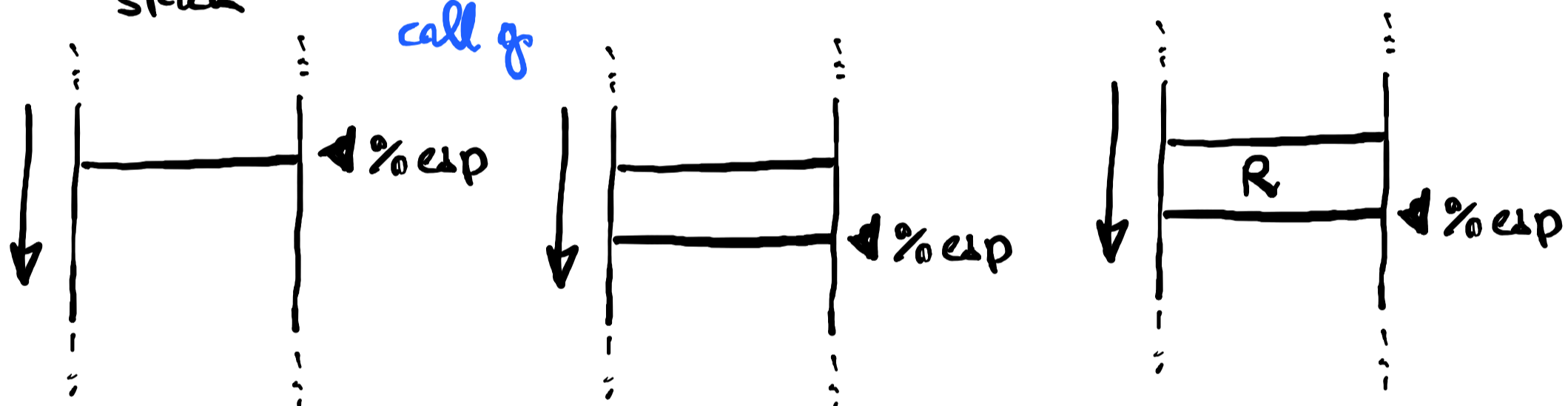
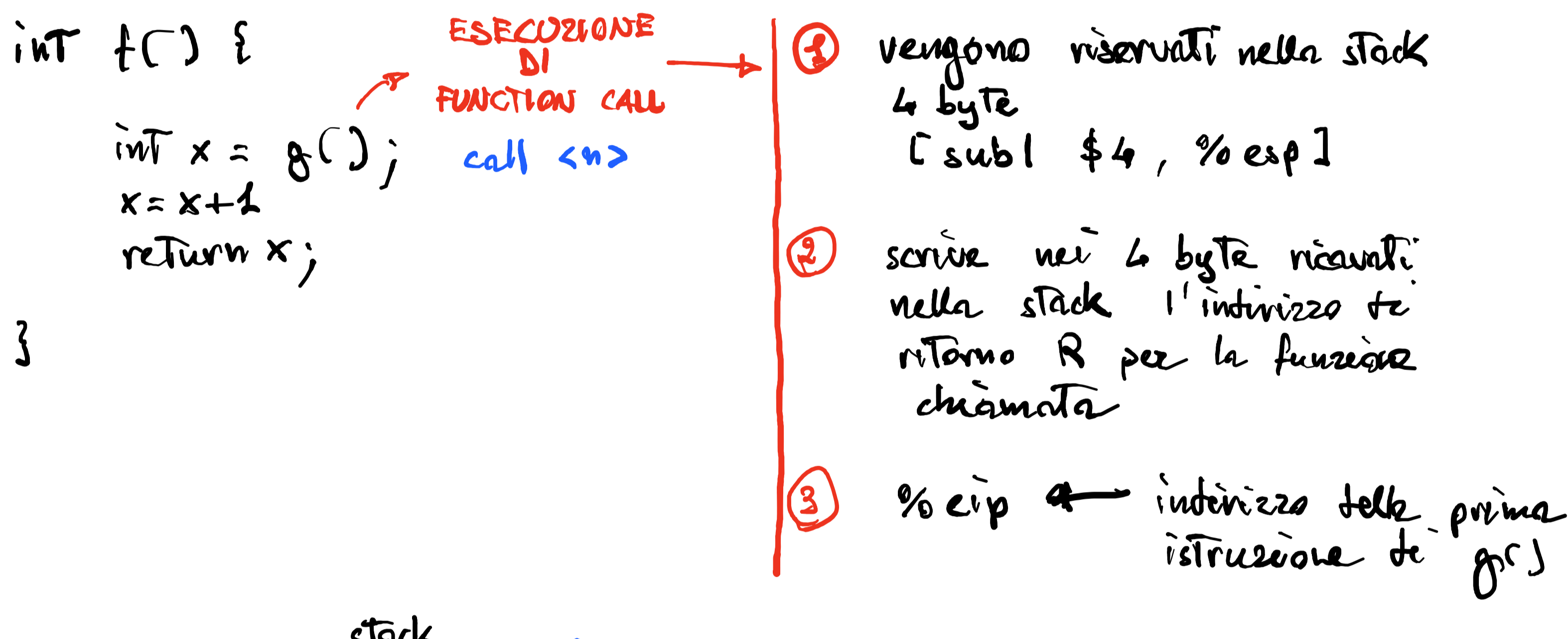


CHIAMATE A FUNZIONE

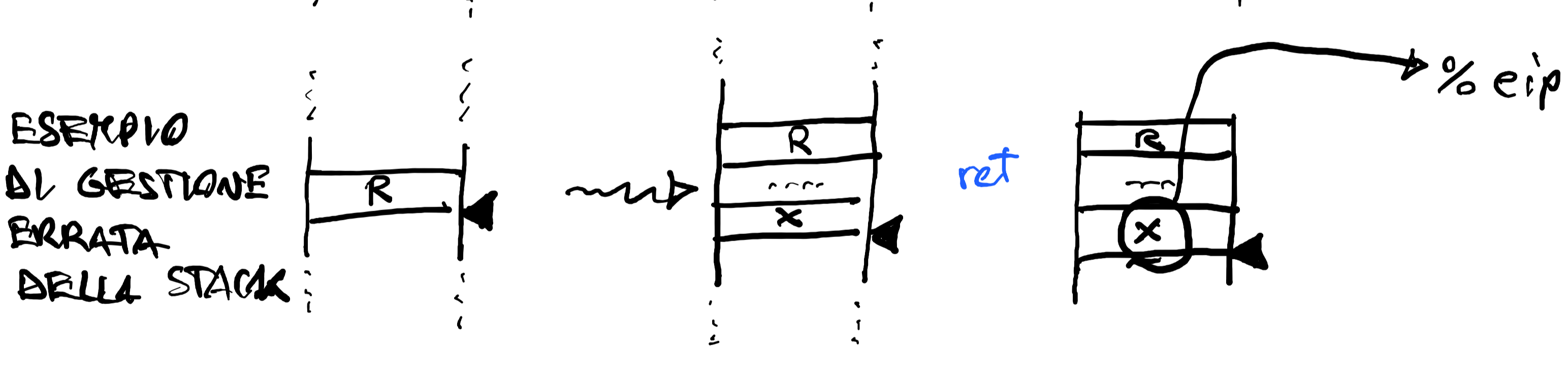
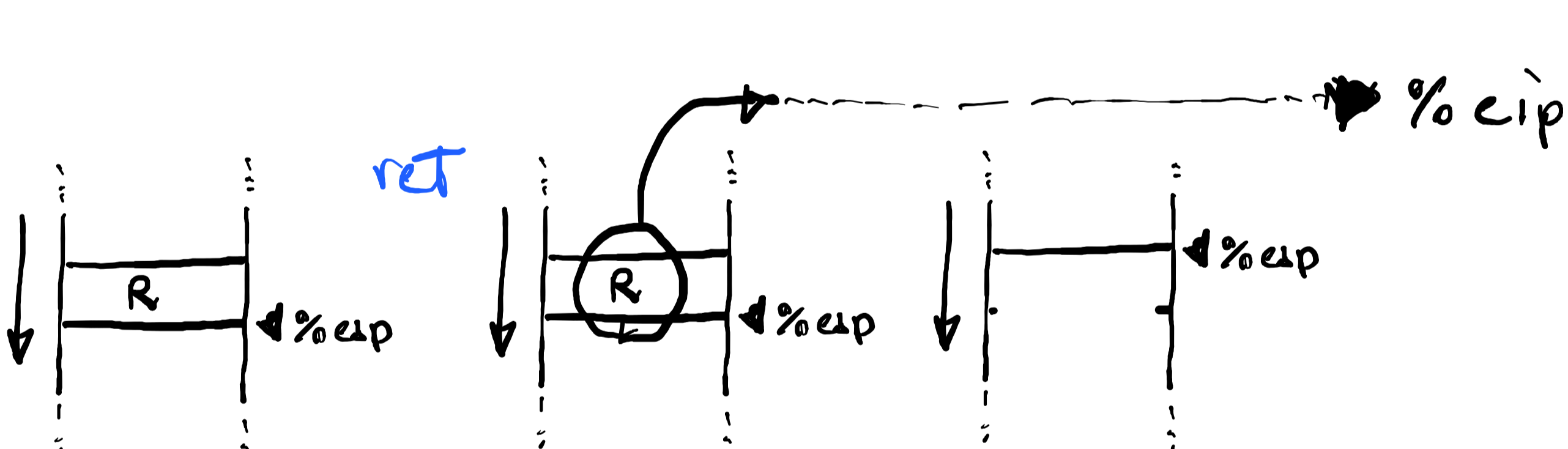


COSA CONTIENE IL FRASE DI ATTIVAZIONE DI F?

- 1) copie dei registri {ebx, edi, esi, ebp}
- 2) variabili locali
- 3) parametri per le funzioni chiamate
- 4) indirizzo di ritorno della funzione chiamata



- RITORNO A FUNZIONE CHIAMANTE ret
- 1) legge da %esp h bytes (R)
 - 2) dealloca 4 byte dallo stack [addl \$4, %esp]
 - 3) %eip ← R

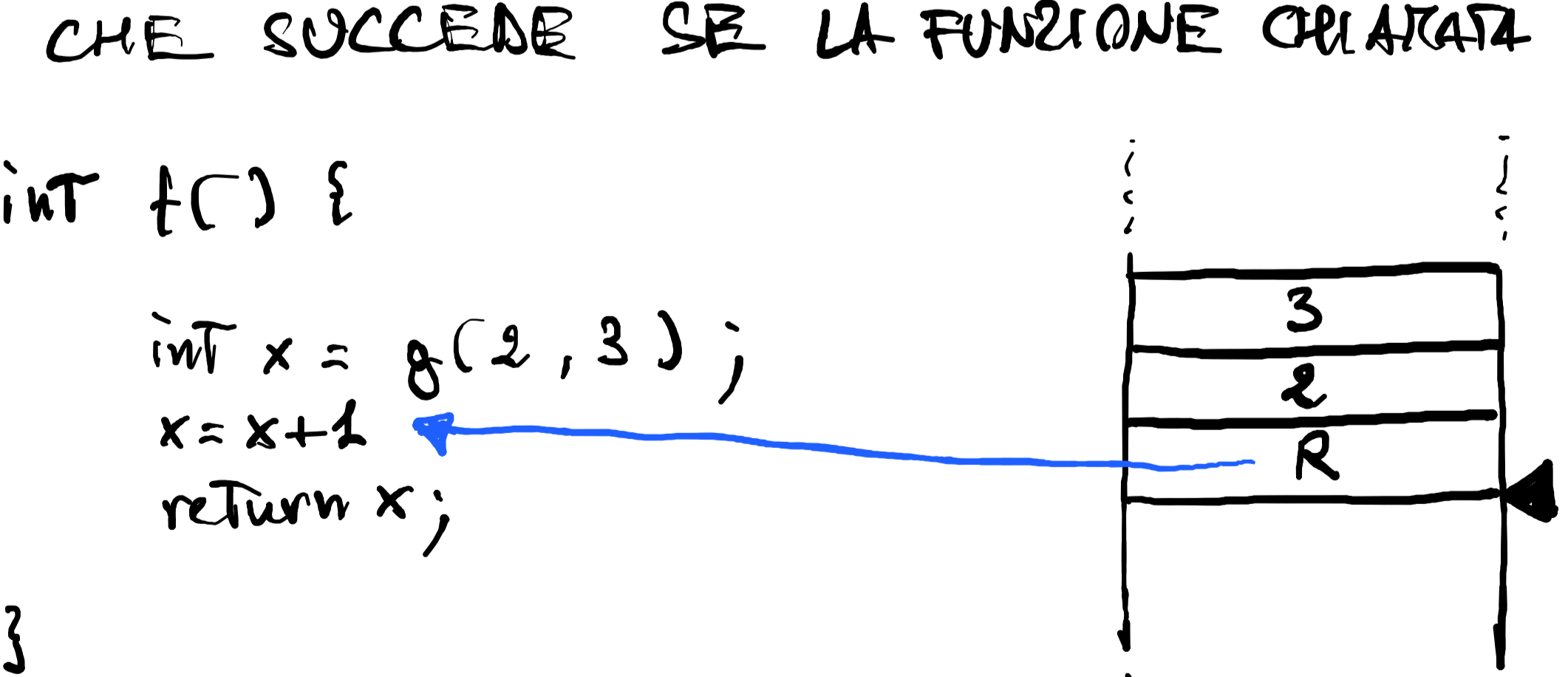


PRIMA DI CHIAMARE RET IL VALORE DI %esp DEVE ESSERE UGUALE A QUELLO CHE AVEVA ALL' INIZIO DELL' ESECUZIONE DELLA FUNZIONE STESSA

```
int f() {
    int x = g();
    x = x + 1;
    return x;
}

.globl f
f:
    call g
    incl %eax
    ret
```

CHE SUCCEDERE SE LA FUNZIONE CHIAMATA HA PARAMETRI?



PREPARAZIONE STACK CON PARAMETRI

- 1) RISERVARE NELLA STACK SPAZIO PER I PARAMETRI
subl \$8, %esp
4 * num. parametri
- 2) COPIARE I VALORI ATTUALI DEI PARAMETRI NELLA STACK
movl \$2, %esp
movl \$3, 4(%esp)
- 3) CHIAMATA A FUNZIONE
call g

```
int f() {
    int x = g(2, 3);
    x = x + 1;
    return x;
}

.globl f
f:
    subl $8, %esp PROLOGO
    movl $3, 4(%esp)
    movl $2, 4(%esp)
    call g
    incl %eax
    addl $8, %esp EPILOGO
    ret
```