

Arhitectura Sistemelor de Calcul

Laborator - Partea 0x01

Bogdan Macovei
Ruxandra Bălucea
Cristian Rusu

Noiembrie 2021

Cuprins

1	Stiva	2
2	Proceduri in limbaj de asamblare	4
2.1	Apelul unei proceduri	5
2.2	Argumentele unei proceduri	5
2.3	Crearea cadrului de apel	7
2.4	Registrii callee si caller saved	9
2.5	Returnarea valorilor	11
3	Apelul functiilor din C	12
3.1	Apelul functiei <code>printf</code>	12
3.2	Apelul functiei <code>scanf</code>	14
3.3	Un exemplu de citire si de afisare a unui graf neorientat	15
4	Resurse suplimentare	18

1 Stiva

Stiva este o regiune dinamică în cadrul unui proces care funcționează pe principiul LIFO (Last In – First Out). La fiecare apel de funcție, este alocată o zonă de memorie pe stivă în care vor fi stocate argumentele funcției, variabilele locale și adresa de retur. La fiecare alocare stiva va crește "în jos", spre adrese mici, așa cum este prezentat și în figura 1.

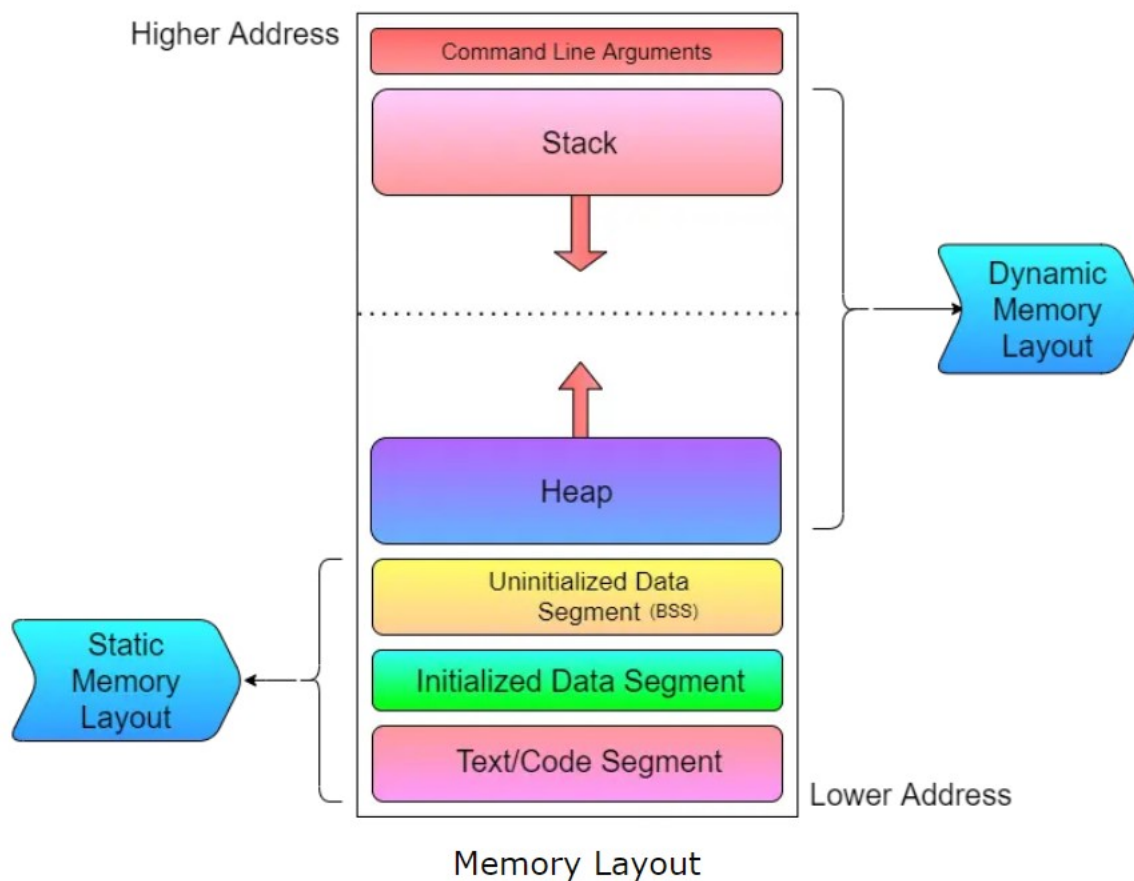


Figura 1: Spațiul de adresă al unui proces¹

Pentru operarea cu stiva, există două instrucțiuni în x86:

push operand

unde **operand** poate fi o constantă, un registru sau o adresă de memorie. Este folosită pentru adăugarea pe stivă;

pop operand

¹Memory Layout, <https://hackthedeveloper.com/memory-layout-c-program/>

unde **operand** poate fi un **registru** sau o **adresa de memorie**. Este folosita pentru scoaterea de valori de pe stiva.

Observatie: Pot fi adaugate pe stiva doar **word-uri** și **long-uri**.

Stack pointer-ul %esp este registrul care indică întotdeauna spre **vârful stivei** și prin care se efectueaza, de fapt, **push-urile** si **pop-urile**. De exemplu, la fiecare **pushl** efectuat, **%esp** creste cu 4 si este **salvata o valoare** relativ la adresa de memorie indicata de **%esp**. Pentru fiecare **popl** efectuat, **valoarea** din varful stivei este **depozitata** in operandul instructiunii, iar **%esp** scade cu 4.

Urmarind scrierea studiata in laboratorul trecut **a(b, c, d)** , valoarea efectiva din **varful stivei** este data de **0(%esp)**. In plus, trebuie remarcat ca varful stivei va indica intotdeauna spre **ultimul byte** al **ultimului element** adăugat pe stiva.

Observatie: Pentru **long-uri** se vor aloca spatii de 4 bytes, iar pentru **word-uri** de 2 bytes. O succesiune de incarcare a 2 word-uri consecutive va ocupa doar 4 octeti. Totuși o incarcare de tip **word** urmata de una de tip **long** va ocupa 8 octei intrucat se doreste mentinerea alinierii pe 32 de biti.

Base pointer-ul este registrul care indică întotdeauna spre **baza stivei** și prin care se va face delimitarea cadrelor de apel și **accesarea elementelor** corespunzătoare acestora.

In continuare este prezentat un exemplu pentru evaluarea expresiei

$$((x + y) * (x - y) * (x + z)) / (y + z)$$

folosind stive. x, y, z sunt 3 numere de tip long declarate global.

```
.data
x: .long 2
y: .long 1
z: .long 3
e: .space 4
.text
.globl _start
_start:

movl y, %eax
addl z, %eax
pushl %eax
; %esp: (y + z)

movl x, %eax
addl z, %eax
pushl %eax
; %esp: (x + z), (y + z)

movl x, %eax
subl y, %eax
pushl %eax
```

```

; %esp: (x - y), (x + z), (y + z)

movl x, %eax
addl y, %eax
pushl %eax
; %esp: (x + y), (x - y), (x + z), (y + z)

popl %eax
popl %ebx
mull %ebx

pushl %eax
; %esp: (x + y) * (x - y), (x + z), (y + z)

popl %eax
popl %ebx
mull %ebx

pushl %eax
; %esp: (x + y) * (x - y) * (x + z), (y + z)

popl %eax
popl %ebx
divl %ebx

pushl %eax
; %esp: ((x + y) * (x - y) * (x + z)) / (y + z)

popl e

mov $1, %eax
xor %ebx, %ebx
int $0x80

```

Observatie: Atentie la comentariile din codul de mai sus! Ca si pana acum, in functie de ce environment utilizati, comentariile pot fi introduse ori cu #, ori cu //;

2 Proceduri in limbaj de asamblare

Daca o prelucrare trebuie facuta de mai multe ori in acelasi fel (eventual cu alte date), in loc sa rescriem grupul respectiv de instructiuni de mai multe ori in program putem sa-l incapsulam intr-o procedura si de fiecare data cand avem nevoie de el sa apelam procedura (eventual cu noile date transmise ca parametri).

In x86 procedurile nu au un mod specific de definire. Ele sunt simple blocuri de cod apelate in sa intr-o maniera specifica. Evident, ele trebuie declarate in zona **.text** si sunt identificate printr-un nume sub forma unei etichete.

2.1 Apelul unei proceduri

Mecanismul de control privind salturile într-o procedură și revenirea în locul de unde a fost apelată este realizat prin două instrucțiuni - **call** și **ret**.

call proc

unde **proc** este eticheta ce marchează începutul procedurii. Prin această instrucțiune se **apelează procedura **proc**** și se **retine adresa de întoarcere** (locul de unde procedura a fost apelată). De fapt, se produce o salvare pe stivă a valorii din **%eip (instruction pointer)** care reține fix adresa instrucțiunii următoare. În același timp, **%eip** preia adresa primei instrucțiuni din **procedura**, realizându-se astfel continuarea execuției din acel punct.

ret

Această instrucțiune realizează un **salt la adresa din varful stivei**. Cum pe parcursul procedurii apelate toate elementele adăugate pe stivă sunt și eliminate, la final în varful stivei se va afla chiar adresa de retur reținută prin instrucțiunea **call**.

O schiță simplistă este prezentată în continuare.

```
.data
.text

proc1:

    ; push-uri și pop-uri în număr egal

    ret ; stivă arată că la intrare în procedură,
        ; în varf se afla deci adresa lui mov %1, %eax
        ; salt la adresa din varf

.globl _start
_start:

    call proc1 ; este adăugată pe stivă adresa lui mov %1, %eax
                ; salt la proc

    mov $1, %eax
    xor %ebx, %ebx
    int $0x80
```

2.2 Argumentele unei proceduri

În continuare, pentru a transmite argumentele unei proceduri, acestea vor fi depozitate tot pe stivă. Datorită conceptului pe care îl implementează o stivă - LIFO (Last In, First Out) este necesar ca argumentele să fie stocate pe stivă în **ordine inversă** pentru a putea fi accesate în ordine naturală. Pe cazul general, considerăm următorul apel **proc(arg1, arg2, ..., argn)**. Schiță pentru apel este următoarea.

```

pushl argn
pushl arg(n-1)
...
pushl arg1
call proc
popl %eax
popl %eax
...
popl %eax
; n pop-uri corespunzatoare celor n argumente

```

Observatie: Toate argumentele incarcate pe stiva, trebuie eliminate la iesirea din procedura.

Exemplu: Fie acum functia **add** avand declaratia **add(x,y,&s)** care realizeaza adunarea a doi intregi **x** si **y** si depoziteaza suma in **s**. Pana in acest punct, un program minimalist in care se cheama respectiva functie cu argumentele **2**, **3**, respectiv adresa unei variabile din memorie, este prezentat mai jos.

```

.data
x: .long 2
y: .long 3
s: .space 4
.text

add:
    movl 4(%esp), %eax
    addl 8(%esp), %eax
    movl 12(%esp), %ebx
    movl %eax, 0(%ebx)

    ret

.globl _start
_start:

    pushl $s
    pushl y
    pushl x
    call add
    popl %edx
    popl %edx
    popl %edx

    mov $1, %eax
    xor %ebx, %ebx
    int $0x80

```

Cerinta: Rulati cu debuggerul si observati evolutia stivei. Explicati indicii de accesare si modul prin care este transmis un parametru cu referinta.

Observatie: Indicii de accesare sunt crescatori, ordinea argumentelor fiind cea descrisa in enunt.

2.3 Crearea cadrului de apel

In exemplul anterior a fost folosit pentru accesare elementelor de pe stiva registrul `%esp`. Totusi aceasta modalitate de lucru poate deveni foarte rapid incomoda daca pe parcursul procedurii apelate este repetat un numar de instructiuni de **push** si **pop**. Dupa fiecare astfel de operatie ar trebui ca programatorul sa regandiasca asezarea de pe stiva si sa schimbe modul de accesare. Practic e posibil ca un acelasi element sa fie accesat o data ca `0(%esp)`, iar dupa adaugarea unei alte valori pe stiva sa fie accesat ca `4(%esp)`. Intrucat dorim sa mentim constanta in modul in care ne raportam la valori de pe stiva, ne vom raporta la registrul `%ebp`, depre care stiam ca memoreaza baza stivei.

Anterior, a fost mentionat, de asemenea, ca pentru fiecare apel de functie se alocă o zonă de memorie pe stivă care este golită la ieşirea din funcţie. O astfel de zonă se numeşte **stack frame** si practic delimiteaza zona apartinand unei proceduri. Pentru procedura curenta, varful stack frame-ului va fi reprezentat de valoarea lui `%esp`. Am dori sa avem si o marcare a bazei acestei zone, iar numele ne trimite direct cu gandul la `%ebp`. Ar fi ideal ca la executia in procedura curenta, `%ebp` sa indice baza zonei proprii de memorii de pe stiva si nu baza intregii stive care nu ar fi de folos intrucat nu suntem interesati de toate **stack frame**-urile create anterior din diverse apeluri imbricate.

Pentru aceasta la fiecare creare de cadru de apel, registrul `%ebp` va fi modificat pentru a indica baza **stack frame-ului** curent. Totusi acesta nu este un pas suficient pentru ca la revenirea din procedura, ne-am dori ca `%ebp` sa indice catre baza **stack frame-ului** procedurii apelante. Atunci o solutie evidenta este sa memoram valoarea initiala la intrarea in procedura si sa o restauram la iesire pentru a se mentine in registrul `%ebp` valoarea corespunzatoare a cadrului in orice moment al executiei.

Astfel, un cadru corect de apel pentru schema din subsectiunea 2.1 este urmatorul:

```
.data
.text

proc1:
    pushl %ebp
    movl %esp, %ebp

    ; codul din corpul procedurii

    popl %ebp
    ret

.globl _start
_start:

    call proc1
```

```

mov $1, %eax
xor %ebx, %ebx
int $0x80

```

Asadar, vom rescrie exemplul din subsectiunea 2.2 raportat la noile cunostinte. Pentru aceasta sa vedem cum arata stiva.

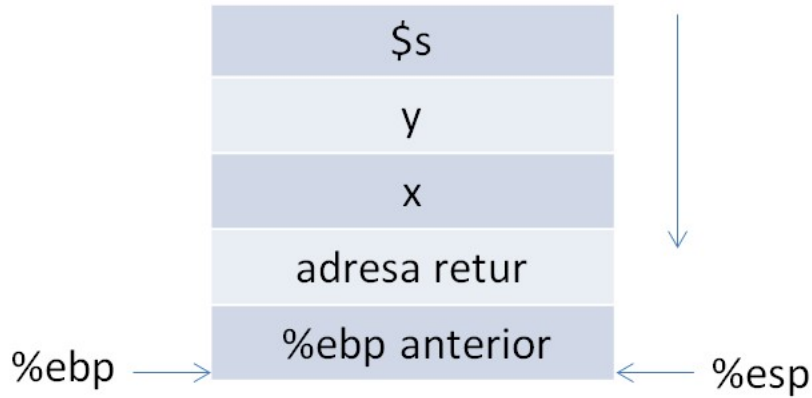


Figura 2: Stiva program subsectiunea 2.2

In acest context, in cadrul functiei **add** putem adauga oricate elemente dorim in jos in stiva pentru ca **%ebp** va ramane fix, singurul care isi modifica valoarea fiind **%esp**. Astfel, programul va fi rescris ca in exemplul de mai jos.

Exemplu:

```

.data
x: .long 2
y: .long 3
s: .space 4
.text

add:
    pushl %ebp
    mov %esp, %ebp

    movl 8(%ebp), %eax
    addl 12(%ebp), %eax
    movl 16(%ebp), %ebx
    movl %eax, 0(%ebx)

    popl %ebp
    ret

.globl _start
_start:

```



```

pushl $s
pushl y
pushl x

call add

popl %edx
popl %edx
popl %edx

mov $1, %eax
xor %ebx, %ebx
int $0x80

```

Cerinta: Rulati cu debuggerul si observati din nou evolutia stivei, precum si noii indici de accesare.

Observatie: Variabilele locale din proceduri se salveaza tot pe stiva in **continuarea cadrului** descris anterior.

2.4 Registrii **callee si caller saved**

Dupa cum bine stim, pe arhitectura x86 numarul de registri este limitat. Am considerat abuziv pana acum ca printr-o analogie cu C-ul, registrii pot fi vazuti ca niste variabile ale programului. In acest caz, urmand aceeasi analogie, vom considera cazul in care avem o variabila **x** declarata in **main** si o variabila cu acelasi nume intr-o procedura apelata. Este bine-cunoscut ca practic cele 2 variabile nu se influenteaza una pe cealalta. Modificarea variabilei **x** din procedura nu are niciun efect asupra celei din **main**. In acelasi mod, trebuie ca registrii modificati intr-o procedura sa nu produca efecte secundare asupra utilizarii lor din apelant. Dorim sa regasim dupa intoarcerea din procedura, in toti registri folositi valorile depozitate inainte de apel.

Pentru aceasta avem din nou ca instrument principal stiva. Astfel in functie de locul in care sunt salvate valorile registrilor, exista 2 tipuri de registri:

- **callee-saved** : **%ebx, %esp, %ebp, %esi, %edi**. Valorile acestor registri se garanteaza a fi restaurate de catre procedura, adica acestea trebuie salvate in zona de variabile locale de catre procedura.
- **caller-saved** : **%eax, %ecx, %edx**. Nu este garantata restaurarea lor. Apelantul trebuie sa salveze aceste valori inainte de incarcarea argumentelor functiei daca doreste sa regaseasca valorile initiale la iesirea din functie.

In cele din urma, asadar, un cadru de apel va arata ca in figura 3

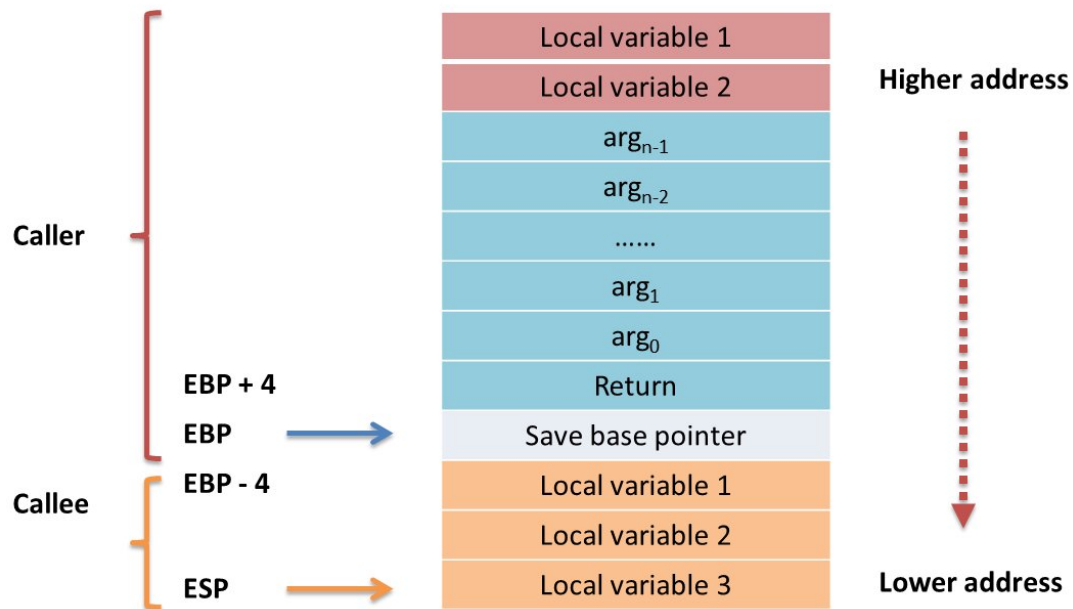


Figura 3: Cadru de apel²

Exemplu: Sa luam acum acelasi cod pentru apelul functiei **add** si sa presupunem ca dupa apel exista o bucata de cod suplimentara care se asteapta sa reagaseasca in registrii **%eax** si **%ebx** valorile de dinainte de apel. O rescriere este prezentata in continuare.

```
.data
x: .long 2
y: .long 3
s: .space 4
.text

add:
    pushl %ebp
    mov %esp, %ebp

    pushl %eax

    movl 8(%ebp), %eax
    addl 12(%ebp), %eax
    movl 16(%ebp), %ebx
```

²Cadru de apel, <https://ocw.cs.pub.ro/courses/iocla/laboratoare/laborator-09>

```

    movl %eax, 0(%ebx)

    popl %eax

    popl %ebp
    ret

.globl _start
_start:

    movl $5, %eax
    movl $6, %ebx

    pushl %ebx
    pushl $s
    pushl y
    pushl x
    call add

    popl %edx
    popl %edx
    popl %edx
    popl %ebx

    eticheta:

    ; cod suplimentar

    mov $1, %eax
    xor %ebx, %ebx
    int $0x80

```

Cerinta: Rulati cu debuggerul si observati din nou evolutia stivei, precum si valorile registrilor %eax, %ebx inainte de inceperea bucatii de cod suplimentare.

2.5 Returnarea valorilor

Pana acum, am considerat numai proceduri care nu returnau nicio valoare. In cazul in care se doreste returnare, valorile vor fi depozitate in aceasta ordine in functie de numarul lor in %eax, %ecx, %edx si ulterior prin varful stivei.

Observatie: Registrii prin care se face returul sunt exact registrii care nu sunt restaurati de apelat. Totusi, si ei pot fi restaurati la un anumit punct in program daca valorile initiale erau necesare apelantului. Asadar, valorile returnate trebuie utilizate (sau memorate) inaintea unei astfel de instructiuni de restaurare a vechii valori.

Cerinta: Modificati ultimul program astfel incat procedura **add** sa aiba doar doi parametri si sa returneze suma in programul principal. Suma va fi ulterior incarcata in memorie la adresa lui **s**.

3 Apelul functiilor din C

Pentru a putea interactiona intr-un program dezvoltat in limbaj de asamblare cu functii din limbajul C, putem utiliza, in loc de *link*-area prezentata in primul suport de laborator, **compilatorul gcc**. In aceasta maniera, putem folosi functiile predefinite in biblioteca standard, printre care si cele mentionate anterior, si anume **printf**, **scanf** si **fflush**.

3.1 Apelul functiei **printf**

In limbajul C, functia **printf** este definita ca avand un numar variabil de argumente, primul fiind **formatul string-ului** de afisat. De exemplu, apeluri valide sunt urmatoarele:

```
printf("Numarul de afisat este: %d\n", x);
printf("Suma numerelor %d si %d este %d\n", x, y, sum);
printf("Numele studentului cu cea mai mare medie este %s\n", nume);
```

Doua dintre formatele utile pe care le vom utiliza sunt

- **%d** - pentru afisarea **intregilor**;
- **%s** - pentru afisarea **sirurilor de caractere**.

Numarul argumentelor pe care le ia **printf** este dat de cate formate speciale utilizam in cadrul primului argument - de exemplu, pentru ca in sirul pentru afisarea sumei de la exemplul anterior avem trei aparitii ale lui **%d**, inseamna ca numarul de argumente va fi egal cu 1 (sirul de format) + cate un argument pentru fiecare valoare care trebuie completata $(3) = 4$.

Pentru a apela functia **printf** intr-un program dezvoltat in limbaj de asamblare, vom proceda astfel: (presupunem ca urmatorul fisier este denumit **call_printf.asm**):

```
.data
    x: .long 23
    formatString: .asciz "Numarul de afisat este: %d"
.text

.global main

main:
    ; incarcam argumentele in ordinea inversa limbajului C
    ; pentru printf("Numarul de afisat este: %d", x);
    ; incarcam x, apoi sirul de format
    pushl x
    pushl $formatString

    ; apeland functia printf
    call printf

    ; pentru fiecare push facut, facem un pop
    ; alegand un registru pe care nu-l utilizam
    popl %ebx
```

```

popl %ebx

movl $1, %eax
xorl %ebx, %ebx
int $0x80

```

Observatii importante:

- pentru ca `printf` acceseaza argumentele in ordinea naturala - mai intai formatul sirului de afisat, apoi argumentele, in ordinea in care apar si in format, inseamna ca le vom incarca in **ordine inversa** pe stiva;
- formatul sirului **nu** se da ca valoare, ci **ca adresa in memorie**, de aceea trebuie ca numele lui sa fie prefixat de simbolul `$`;
- pentru a face `pop`, putem utiliza orice registru care nu contine, momentan, o valoare pe care vrem sa o pastram - `pop` modifica accesul pe care il are registrul `%esp` (*stack pointer*-ul) asupra stivei, si descarca valoarea actuala din *top* in registrul pe care noi il precizam. In acest caz, am ales sa facem descarcarea in `%ebx`, fiind echivalent orice alt registru;
- instructiunea `xorl %ebx, %ebx` este echivalenta cu instructiunea `movl $0, %ebx`.

Pentru a compila programul, vom utiliza compilatorul `gcc`:

```

as --32 call_printf.asm -o call_printf.o
gcc -m32 call_printf.o -o call_printf
./call_printf

```

Cel mai probabil, in acest moment nu vom avea o valoare efectiva afisata la **standard output**, din cauza modului in care sunt implementate sistemele de operare. Pentru a obliga **afisarea buffer-ului curent de memorie**, vom utiliza functia `fflush` cu argumentul `NULL`. Apelul este foarte simplu, trebuie sa incarcam pe stiva `NULL`, adica valoarea 0, si sa o descarcam, din nou, intr-un registru pe care nu-l avem momentan completat cu o valoare utila - sa presupunem ca tot `%ebx`. Apelul va fi:

```

pushl $0
call fflush
popl %ebx

```

In acest moment, exemplul complet va avea urmatoarea forma:

```

.data
    x: .long 23
    formatString: .asciz "Numarul de afisat este: %d"
.text

.global main

main:
    pushl x
    pushl $formatString
    call printf

```

```

    popl %ebx
    popl %ebx

    pushl $0
    call fflush
    popl %ebx

    movl $1, %eax
    xorl %ebx, %ebx
    int $0x80

```

Vom compila iar:

```

as --32 call_printf.asm -o call_printf.o
gcc -m32 call_printf.o -o call_printf
./call_printf

```

Care, de aceasta data, va afisa corect pe ecran mesajul

Numarul de afisat este: 23

Observatie. Pentru a standardiza modul in care vom face *call*-urile catre `printf`, vom avea mereu un `printf` urmat de un `fflush`.

3.2 Apelul functiei scanf

Vom pleca, din nou, de la modul in care aceasta functie este apelata in limbajul C, si anume:

```

scanf("%d", &x);
scanf("%d %d", &x, &y);

```

Desi apelul seamana foarte mult cu cel pe care il utilizam pentru `printf`, observam ca, de aceasta data, argumentele nu mai sunt date prin valoarea propriu-zisa - nu apelam `x`, ci `&x`. Acest lucru trebuie sa se reflecte si in limbajul de asamblare. Pentru aceasta, avem simbolul `$`, care ne da acces la locatia de memorie a unei variabile declarate in sectiunea `.data`.

Vom demonstra aceste lucruri prin intermediul codului de mai jos, presupus salvat intr-un fisier de forma `call_scanf.asm`, pentru citirea unui intreg de la tastatura.

```

.data
    x: .space 4 ; nu stim momentan valoarea citita, dar stim cat ocupa
    formatString: .asciz "%d"
.text

.global main

main:
    ; incarcam in stiva NU x, ci ADRESA lui x
    ; adica nu x, ci &x
    pushl $x
    ; incarcam adresa formatului

```

```

pushl $formatString
call scanf
; descarcam ce am incarcato in stiva
popl %ebx
popl %ebx

movl $1, %eax
xorl %ebx, %ebx
int $0x80

```

3.3 Un exemplu de citire si de afisare a unui graf neorientat

Pentru a demonstra utilizarea pentru printf, scanf si fflush, vom prezenta citirea unui graf neorientat, dat prin numarul de varfuri, numarul de muchii si muchiile acestuia.

```

.data
    matrix: .space 1600
    columnIndex: .space 4
    lineIndex: .space 4
    n: .space 4
    nrMuchii: .space 4
    index: .space 4
    left: .space 4
    right: .space 4
    formatScanf: .asciz "%d"
    formatPrintf: .asciz "%d "
    newLine: .asciz "\n"

.text

.global main

main:
    pushl $n
    pushl $formatScanf
    call scanf
    popl %ebx
    popl %ebx

    pushl $nrMuchii
    pushl $formatScanf
    call scanf
    popl %ebx
    popl %ebx

; simulam, de fapt
; for (int index = 0; index < nrMuchii; index++)
; {
;     scanf("%d", &left);

```

```

;         scanf("%d", &right);
;         matrix[left][right] = 1;
;         matrix[right][left] = 1;
;     }
    movl $0, index
et_for:
    movl index, %ecx
    cmp %ecx, nrMuchii
    je et_afis_matr

    pushl $left
    pushl $formatScanf
    call scanf
    popl %ebx
    popl %ebx

    pushl $right
    pushl $formatScanf
    call scanf
    popl %ebx
    popl %ebx

; trebuie sa completez
; matrix[left][right] = 1
; indexul este left * n + right

    movl left, %eax
    movl $0, %edx
    mull n
; %eax := left * n
    addl right, %eax
; %eax := left * n + right

    lea matrix, %edi
    movl $1, (%edi, %eax, 4)

; trebuie sa completez matrix[right][left] = 1
; indexul este right * n + left

    movl right, %eax
    movl $0, %edx
    mull n
; %eax := right * n
    addl left, %eax
; %eax := right * n + left

    lea matrix, %edi
    movl $1, (%edi, %eax, 4)

```



```

    incl index
    jmp et_for

et_afis_matr:
    movl $0, lineIndex
    for_lines:
        movl lineIndex, %ecx
        cmp %ecx, n
        je et_exit

        movl $0, columnIndex
        for_columns:
            movl columnIndex, %ecx
            cmp %ecx, n
            je cont

            ; afisez matrix[lineIndex][columnIndex]
            ; indexul este lineIndex * n + columnIndex
            movl lineIndex, %eax
            movl $0, %edx
            mull n
            addl columnIndex, %eax
            ; %eax = lineIndex * n + columnIndex

            lea matrix, %edi
            movl (%edi, %eax, 4), %ebx

            pushl %ebx
            pushl $formatPrintf
            call printf
            popl %ebx
            popl %ebx

            pushl $0
            call fflush
            popl %ebx

            incl columnIndex
            jmp for_columns

    cont:
        movl $4, %eax
        movl $1, %ebx
        movl $newLine, %ecx
        movl $2, %edx
        int $0x80

```

```

        incl lineIndex
        jmp for_lines

et_exit:
        movl $1, %eax
        movl $0, %ebx
        int $0x80

```

4 Resurse suplimentare

Pentru mai multe detalii despre GNU Assembly va recomandam cartea *Professional Assembly Language* de Richard Blum si in special urmatoarele capitole:

- Chapter 7: Using numbers subcapitolele SIMD Integers, Floating-Point Numbers;
- Chapter 9: Advanced Math Functions;
- Chapter 11: Using Functions;
- Chapter 12: Using Linux System Calls;
- Chapter 13: Using Inline Assembly;
- Chapter 15: Optimizing Routines;
- Chapter 17: Using Advanced IA-32 Features.