2.6.5. Reprezentarea instrucţiunilor maşină

O instrucţiune maşină x86 reprezintă o secvenţă de 1 până la 15 octeţi, care prin valorile lor specifică o operaţie de executat, operanzii asupra cărora va fi aplicată, precum şi modificatori suplimentari care controlează modul în care aceasta va fi executată.

O instrucţiune maşină x86 are maximum doi operanzi. Pentru cele mai multe dintre instrucţiuni, cei doi operanzi poartă numele de *sursă*, respectiv *destinaţie*. Dintre cei doi operanzi, maximum unul se poate afla în memoria RAM. Celălalt se află fie într-un registru al **EU**, fie este o constantă întreagă. Astfel, o instrucţiune are forma:

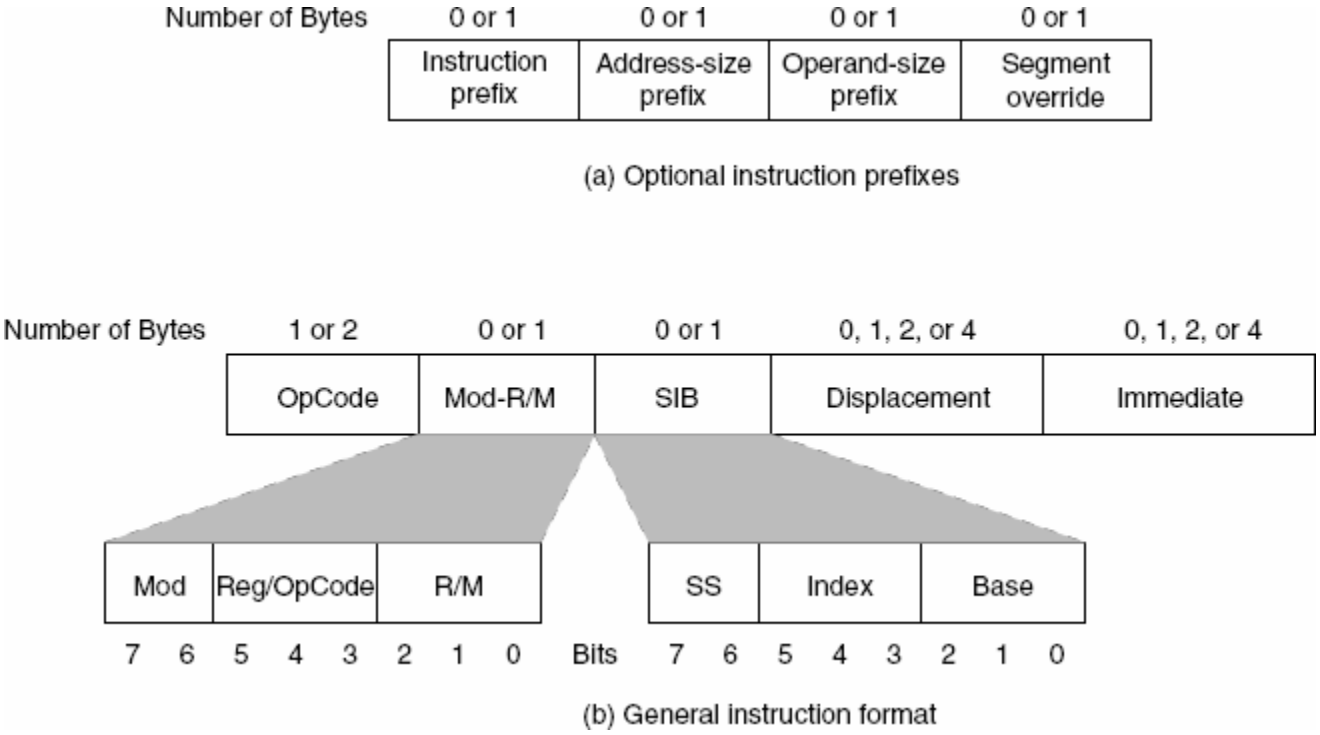
numeinstrucţiune *destinaţie****,*** *sursă*

Formatul intern al unei instrucţiuni este variabil, el putând ocupa între 1 şi 15 octeţi, având următoarea formă generală de reprezentare (*Instructions byte-codes from OllyDbg*):

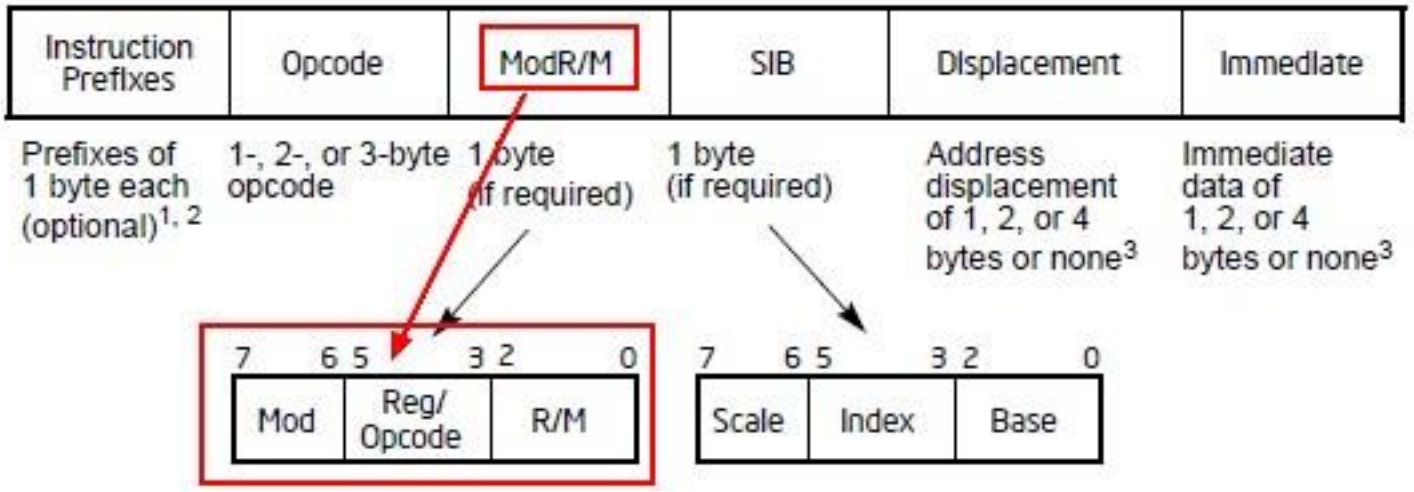
[prefixe] + cod + [ModR/M] + [SIB] + [deplasament] + [imediat]

Prefixele controlează modul în care o instrucţiune se execută. Acestea sunt opţionale (0 până la maximum 4) şi ocupă câte un octet fiecare. De exemplu, acestea pot solicita execuţia repetată (în buclă) a instrucţiunii curente sau pot bloca magistrala de adrese pe parcursul execuţiei pentru a nu permite accesul concurent la operanzi şi rezultate.

Operaţia care se va efectua este identificată prin intermediul a 1 sau 2 octeţi de *cod* (opcode), aceştia fiind singurii octeţi obligatoriu prezenţi, indiferent de instrucţiune.



Although the diagram seems to imply that instructions can be up to 16 bytes long, in actuality the x86 will not allow instructions greater than 15 bytes in length.



Octetul *ModR/M* (mod registru/memorie) specifică pentru unele dintre instrucţiuni natura şi locul operanzilor (registru, memorie). Acesta permite specificarea fie a unui registru, fie a unei locaţii de memorie a cărei adresă este exprimată prin intermediul unui offset (*http://datacadamia.com/intel/modrm*)

Pentru cazuri mai complexe de adresare decât cele codificabile direct prin ModR/M, combinarea acestuia cu octetul SIB (Scale – Index – Base) permite următoarea formulă generală de definire a unui offset:

offset = [bază] + [index × scală] + [constantă]
(SIB) (deplasament + imediat)

unde pentru bază şi index vor fi folosite valorile a doi regiştri iar scală este 1, 2, 4 sau 8. Regiştrii permişi ca bază sau / şi index sunt: EAX, EBX, ECX, EDX, EBP, ESI, EDI. Registrul ESP este disponibil ca bază însă nu poate fi folosit cu rol de index. (http://www.c-jump.com/CIS77/CPU/x86/lecture.html#X77_0100_sib_byte_layout)

Majoritatea instrucţiunilor folosesc pentru reprezentare fie numai campul de cod, fie cod urmat de ModR/M.

Deplasament (displacement) apare în cazul unor forme de adresare particulare (operanzi din memorie) şi urmează direct după ModR/M sau SIB, când SIB este prezent. Acest câmp poate fi codificat fie pe octet, fie pe cuvânt, fie pe dublu cuvant (32 biţi).

The most common addressing mode, and the one that's easiest to understand, is the *displacement-only* (or ***direct***) addressing mode. **The displacement-only addressing mode consists of a 32-bit constant that specifies the address of the target location**. The displacement-only addressing mode **is perfect for accessing simple scalar variables**. Intel named this the displacement-only addressing mode because a 32-bit constant (displacement) follows the MOV opcode in memory. **On the 80x86 processors, this displacement is an offset** from the beginning of memory (that is, address zero).

Displacement mode, **the operand's offset** is contained as part of the instruction as an 8-, 16-, or 32-bit displacement. The displacement addressing mode is found on few machines because, as mentioned earlier, it leads to long instructions. In the case of the x86, the displacement value can be as long as 32 bits, making for a 6-byte instruction. **Displacement addressing can be useful for referencing global variables.**

Ca şi consecinţă a imposibilităţii prezenţei mai multor câmpuri de ModR/M, SIB şi deplasament într-o instrucţiune, arhitectura 80x86 NU permite codificarea a două adrese de memorie în aceeaşi instrucţiune.

Valoare imediată oferă posibilitatea definirii unui operand ca fiind o constantă numerică pe 1, 2 sau 4 octeţi. Când este prezent, acest câmp apare întotdeauna la sfârşitul instrucţiunii.

2.6.6. Adrese FAR şi NEAR

Pentru a adresa o locaţie din memoria RAM sunt necesare două valori: una care să indice segmentul, alta care să indice offsetul în cadrul segmentului. Pentru a simplifica referirea la memorie, microprocesorul derivă, în lipsa unei alte specificări, adresa segmentului din **unul dintre regiştrii de segment CS, DS, SS sau ES**. Alegerea implicită a unui registru de segment se face după nişte reguli proprii instrucţiunii folosite.

Prin definiţie, o adresă în care se specifică doar offsetul, urmând ca segmentul să fie preluat implicit dintr-un registru de segment poartă numele de *adresă NEAR* (adresă apropiată). O adresă NEAR se află întotdeauna în interiorul unuia din cele patru segmente active.

O adresă în care programatorul indică explicit un selector de segment poartă numele de *adresă FAR* (adresă îndepărtată). O adresă FAR este deci o SPECIFICARE COMPLETA DE ADRESA si ea se poate exprima în trei moduri:

- $s_3s_2s_1s_0$: specificare_offset unde $s_3s_2s_1s_0$ este o constantă;
- registru_segment : specificare_offset, registru segment fiind CS, DS, SS, ES, FS sau GS;
- FAR [variabilă], unde variabilă este de tip QWORD şi conţine cei 6 octeţi constituind adresa FAR. (ceea ce numim variabila pointer in limbajele de nivel inalt)

Formatul intern al unei adrese FAR este: la adresa mai mică se află offsetul, iar la adresa mai mare cu 4 (cuvântul care urmează după dublucuvântul curent) se află cuvântul ce conţine selectorul care indică segmentul.

Reprezentarea adreselor respectă principiul reprezentării little-endian expus în capitolul 1, paragraf 1.3.2.3: partea cea mai puţin semnificativă are adresa cea mai mică, iar partea cea mai semnificativă are adresa cea mai mare.

2.6.7. Calculul offsetului unui operand. Moduri de adresare

În cadrul unei instrucţiuni există 3 moduri de a specifica un operand pe care aceasta îl solicită:

- *modul registru*, dacă pe post de operand se află un registru al maşinii; mov eax, 17
- *modul imediat*, atunci când în instrucţiune se află chiar valoarea operandului (nu adresa lui şi nici un registru în care să fie conţinut); mov eax, 17
- *modul adresare la memorie*, dacă operandul se află efectiv undeva în memorie. În acest caz, offsetul lui se calculează după următoarea formulă:

$$\textit{adresa\_offset} = [\text{ bază }] + [\text{ index} \times \text{scală }] + [\text{ constanta }]$$

Deci *adresa_offset* se obţine din următoarele (maxim) patru elemente:

- conţinutul unuia dintre regiştrii EAX, EBX, ECX, EDX, EBP, ESI, EDI sau ESP ca bază;
- conţinutul unuia dintre regiştrii EAX, EBX, ECX, EDX, EBP, ESI sau EDI drept index;
- factor numeric (scală) pentru a înmulţi valoarea registrului index cu 1, 2, 4 sau 8
- valoarea unei constante numerice, pe octet, cuvant sau dublucuvânt.

De aici rezultă următoarele moduri de adresare la memorie:

- *directă*, atunci când apare numai *constanta*;
- *bazată*, dacă în calcul apare unul dintre regiştrii bază;
- *scalat-indexată*, dacă în calcul apare unul dintre regiştrii index;

Cele trei moduri de adresare a memoriei pot fi combinate. De exemplu, poate să apară adresare directă bazată, adresare bazată şi scalat-indexată etc

Adresarea care NU este directa se numeste ***adresare indirecta*** (bazata si/sau indexata). Deci o adresare indirecta este cea pt care avem specificat cel putin un registru intre parantezele drepte.

La instrucţiunile de salt mai apare şi un alt tip de adresare numit adresare *relativă*.

Adresa relativă indică poziţia următoarei instrucţiuni de executat, în raport cu poziţia curentă. Poziţia este indicată prin numărul de octeţi de cod peste care se va sări. Arhitectura x86 permite atât adrese relative scurte (SHORT Address), reprezentate pe octet şi având valori între -128 şi 127, cât şi adrese relative apropiate (NEAR Address), pe dublucuvânt cu valori între -2147483648 şi 2147483647.

```
Jmp MaiJos  ; aceasta instructiune se traduce (vezi OllyDbg) de obicei in Jmp [0084]↓
…….
…….
MaiJos:
   Mov eax, ebx
```