Kaip formuojamas objektinis kodas? [http://goo.gl/462lLw]

Kiekviena mnemonika (MOV, ADD, CLC) gali būti susieta su viena ar daugiau mašininėmis instrukcijomis. 8086 procesoriaus instrukcijų kodai pateikiami prie mokymosi medžiagos.

Panagrinėkime keletą pavyzdžių.

MOV (ištrauka iš oficialios Intel dokumentacijos):

Mnemonic and Description	Instruction Code			
DATA TRANSFER				
MOV = Move:	76543210	76543210	76543210	76543210
Register/Memory to/from Register	100010dw	mod reg r/m		
Immediate to Register/Memory	1100011w	mod 000 r/m	data	data if w = 1
Immediate to Register	1011 w reg	data	data if w = 1	
Memory to Accumulator	1010000w	addr-low	addr-high	
Accumulator to Memory	1010001w	addr-low	addr-high	
Register/Memory to Segment Register	10001110	mod 0 reg r/m		
Segment Register to Register/Memory	10001100	mod 0 reg r/m		

Matome, kad MOV turi 7 variantus. Panagrinkime kai kuriuos.

Pirmas variantas: registras/atmintis <- atmintis/registras arba atvirkščiai.

Pirmas baitas -- instrukcijos kodas jame du jaunesni bitai turi tam tikrą prasmę. Bitas **d** reiškia kryptį: jeigu d=1 yra kryptis yra į registrą, o jeigu 0 - iš registro. Bitas **w** reiškia *ar žodis:* jiegu jis yra nulis, tai turime 8 bitų operandus, o jeigu 1 - 16 bitų.

Antras baitas vadinamas *adresavimo baitu.* Jis pasitaiko labai dažnai ir ne tik MOV instrukcijos atveju. To baito struktūra sudaryta iš trijų laukų:

a) laukas **mod:** dviejų bitų;
b) laukas **reg:** trijų bitų;
c) laukas **r/m:** trijų bitų.

Šie laukai pilnai nusako operandus. Juos galima sužnoti iš lentelių:

Mod kodas	Apibūdinimas
00	Bet kokiam **r/m** atvejui, išskyrus **110**, po komandos NEBUS papildomų POSLINKIO baitų. Kai **r/m** yra 110, tai turime POSLINKĮ [disp-low] [disp-high].
01	Bet kokiam **r/m** atvejui turime ŽENKLINĮ 8 bitų POSLINKĮ, t.y. nuo -128 iki +127.
10	Bet kokiam **r/m** atvejui turime BEŽENKLINĮ 16 bitų POSLINKĮ, t.y. nuo 0000 iki FFFF: [disp-low][disp-high]
11	Abu operandai yra registrai

r/m laukas (Intel dokumentacija):

MOD = 11			EFFECTIVE ADDRESS CALCULATION			
R/M	W = 0	W = 1	R/M	MOD = 00	MOD = 01	MOD = 10
000	AL	AX	000	(BX) + (SI)	(BX) + (SI) + D8	(BX) + (SI) + D16
001	CL	CX	001	(BX) + (DI)	(BX) + (DI) + D8	(BX) + (DI) + D16
010	DL	DX	010	(BP) + (SI)	(BP) + (SI) + D8	(BP) + (SI) + D16
011	BL	BX	011	(BP) + (DI)	(BP) + (DI) + D8	(BP) + (DI) + D16
100	AH	SP	100	(SI)	(SI) + D8	(SI) + D16
101	CH	BP	101	(DI)	(DI) + D8	(DI) + D16
110	DH	SI	110	DIRECT ADDRESS	(BP) + D8	(BP) + D16
111	BH	DI	111	(BX)	(BX) + D8	(BX) + D16

reg laukas:

REG	W = 0	W = 1
000	AL	AX
001	CL	CX
010	DL	DX
011	BL	BX
100	AH	SP
101	CH	BP
110	DH	SI
111	BH	DI

Pavyzdžiai.

1. Užkoduokime instrukciją

mov BX, CX

Turime: instrukcijos kodas yra 1000 10 d w . Kadangi perdavimas eina į registrą, tai d = 1. w=1, nes registrai yra 16 bitų. Taigi, instrukcijos kodas yra **8B** .

Adresavimo baito laukas **mod** yra 11, nes abu operandai yra registrai, **reg** laukas yra 011(žr. lentelę su registrų numeriais), **r/m** laukas yra 001. Gauname: 11 011 001 -> 1101 1001 -> D9.

Pilnas instrukcijos kodas yra 8B D9.

2. Užkoduokime instrukciją

mov [BX], DL

Turime: instrukcijos kodas yra 1000 10 d w . Kadangi perdavimas eina iš registro, tai d = 0. w=0, nes registras yra 8 bitų. Taigi, instrukcijos kodas yra **88** .

Adresavimo baito laukas **mod** yra 00, nes nėra poslinkio, **reg** laukas yra 010(žr. lentelę su registrų numeriais), **r/m** laukas yra 111. Gauname: 00 010 111 -> 0001 0111 -> 17.

Pilnas instrukcijos kodas yra 88 17.

3. Užkoduokime instrukciją

mov SI, [1234]

Turime: instrukcijos kodas yra 1000 10 d w . Kadangi perdavimas eina į registrą, tai d = 1. w=1, nes registras yra 16 bitų. Taigi, instrukcijos kodas yra **8B** .

Adresavimo baito laukas **mod** yra 00 (minėtas išskirtinis atvejis), **reg** laukas yra 110(žr. lentelę su registrų numeriais), **r/m** laukas yra 110. Gauname: 00 110 110 -> 36.

POSLINKIO baitai yra 34 12.

Pilnas instrukcijos kodas yra 8B 36 34 12.

4. Užkoduokime instrukciją

mov DL, [BP]

Turime: instrukcijos kodas yra 1000 10 d w . Kadangi perdavimas eina į registrą, tai d = 1. w=0, nes registras yra 8 bitų. Taigi, instrukcijos kodas yra **8A** .

Adresavimo baito laukas **mod** yra 01, nes kito pasirinkimo (be poslinkio) nėra, **reg** laukas yra 010(žr. lentelę su registrų numeriais), **r/m** laukas yra 110. Gauname: 01 010 110 -> 56.

POSLINKIS yra 00

Pilnas instrukcijos kodas yra 8A 56 00.

Trečias variantas: registras <- konstanta

Šiuo atveju dalis adreso dalyvauja instrukcijos kode.

Pavyzdys.

Užkoduokime instrukciją:

mov CL, -15

Turime: instrukcijos kodas yra 1011 w reg . Laukas **reg** yra 001, bitas **w** yra 0, nes turime reikalą su 8 bitų operandais. Taigi, instrukcijos kodas yra B1.

Konstanta -15 užsirašo kaip EB (prisiminkit 1 užsiėmimą: apie neigiamus skaičius :)).

Galutinis rezultatas yra toks: pilnas kodas yra B1 EB.

Pratimai

1. Užrašykite instrukcijų kodus:
   a) mov AL, [BX+SI+15]
   b) mov AH, [SI-14]
   c) mov CL, [BP+12A4]
   d) mov [BP+1234], 5678
   e) mov al, [9ABC]

2. Panagrinėkite savarankiškai Jums žinomų instrukcijų kodus. Užrašykite iokių instrukcijų kodus:
   a) add BX, CX
   b) sub [BX+1234], DX
   c) push CX
   d) pop DS
   e) ror word ptr [si], 1
3. Disasembliuokit kodą:

```
50 53 81 C3 34 12 5B 58
```