Stekas

- PUSH – 2 baitai (žodinis registras/nurodyta atminties vieta) yra įdedami į steką, prieš tai SP sumažinus 2 vienetais.
  1. SP:=SP-2;
  2. MOV SS:SP, jaunesnysis baitas (arba pirmas baitas iš atminties)
     MOV SS:(SP+1), vyresnysis baitas (arba sekantis baitas iš atminties)
- POP – 2 baitai iš steko yra patalpinami į nurodytą žodinį registrą/atminties vietą, po to SP padidinamas 2 vienetais.
  1. MOV jaunesnysis baitas, SS:SP
     MOV vyresnysis baitas, SS:(SP+1)
  2. SP:=SP+2;

Pavyzdinis uždavinys su steku (1)

AX=9876, SS=4567, SP=1973. Vykdoma komanda PUSH AX. Kokia baito, kurio absoliutus adresas atmintyje yra 46FE2h, reikšmė?

- Reikės ieškoti baito reikšmės atmintyje → pasibraižom atmintį.
- Vykdom komandą PUSH AX:
  1. SP:=1973-2=1971.
  2. MOV SS:SP, 76h (*į atminties vietą, kurios AA yra 4567:1971, patalpinom baitą, kurio reikšmė 76h*)
     MOV SS:(SP+1), 98h (*į atminties vietą, kurios AA yra 4567:1972 patalpinom baitą, kurio reikšmė yra 98h*)
- Įvykdėm PUSH - atsinaujinam atminties lentelę.

SP	Baito reikšmė
1969	XX
1970	XX
1971	XX
1972	XX
1973	XX

Atminties dalis prieš PUSH

SP	Baito reikšmė
1969	XX
1970	XX
1971	76
1972	98
1973	XX

Atminties dalis po PUSH

Pavyzdinis uždavinys su steku (2)

- Atminties vieta, kuri yra duota uždaviny: 47642h
- Reik patikrinti, galbūt mūsų turima atminties vieta yra ta pati, kurios ir reikia:
  1. AA=seg_reg_reikšmė*10h+EA
  2. Turim steką dalį, vadinasi, galim rasti tos dalies absoliučius adresus: SS*10h+SP (imam dabartinį SP, kuris yra 1971)
  3. 4567*10+1971 = 46FE1h
- Atsinaujinam lentelę (užsirašom ir absoliučius adresus)
- Pastebim, kad baito, kurio absoliutus adresas atmintyje yra 46FE2, reikšmė yra 98h

Absoliutus adresas	**SP**	**Baito reikšmė**
46FDF	1969	XX
46FE0	1970	XX
46FE1	1971	76
46FE2	1972	98
46FE3	1973	XX

Atmintis su absoliučiais adresais

<u>Ats.: 98h</u>

Valdymo perdavimo komandos

Valdymo perdavimas – toliau vykdomas ne kodas, einantis atmintyje po einamosios komandos, o iš bet kurios nurodytos atminties vietos.
Valdymo perdavimo komandos:

1. **Sąlyginės**. Valdymas bus perduotas tik tuomet, jei bus patenkinta tam tikra sąlyga (*pvz.: JE narnia, LOOP hogwarts*).
2. **Besąlyginės**. Valdymas bus perduotas į nurodytą vietą netikrindamas jokių sąlygų (*pvz.: JMP hell*).

Besąlyginis valdymo perdavimas (1)

Komandos: JMP, CALL, RET, INT, IRET

Besąlyginis valdymo perdavimas gali būti: vidinis/išorinis + tiesioginis/netiesioginis/artimas.

- **Vidinis:** valdymas yra perduodamas segmento viduje (*keičiasi tik IP reikšmė*)
- **Išorinis:** valdymas yra perduodamas visos atminties ribose (*keičiasi ir IP, ir CS reikšmės*)

Besąlyginis valdymo perdavimas (2)

- **Tiesioginis** – nauja IP reikšmė (arba nauja IP ir CS reikšmės) imama **tiesiogiai iš vykdomo kodo**, t.y., jos yra tam tikri baitai po komandos OPK. *Pvz.: E9 F9 FF → IP:=IP_komandos_vykdymo_metu + FFF9*
- **Netiesioginis –** nauja IP reikšmė (arba nauja IP ir CS reikšmės) **randama naudojant adresavimo baitą**. Operandas atmintyje parodo, iš kur reikės pasiimti naują IP (arba CS ir IP) reikšmę. Jei mod=11, tai IP = žodinio registro (kurį nurodo r/m) reikšmė. Pastaba: netiesioginio valdymo perdavimo atveju adresavimo baito reg dalis yra OPK plėtinys. *Pvz.: FF 68 FD → analizuojam adresavimo baitą 68 ir naują IP pasiimam iš atminties vietos, kurią nurodė mod + r/m kombinacija*
- **Artimas –** tiesioginio tipas, kai valdymas perduodamas mažu atstumu [-128;127 baitai], todėl poslinkis užrašomas vienam baite. Pastaba: negalimas išorinis artimas atvejis. *Pvz.: EB EC → IP:=IP_komandos_vykdymo_metu+FFEC*

Besąlyginis valdymo perdavimas (3)

<table>
<tr><td>Vidinis artimas</td><td colspan="2">1. Iš mašininio kodo po OPK imamas 1 baito poslinkis.
2. Baitas išplečiamas pagal plėtimo pagal ženklą taisyklę.
3. IP:= gautas_rezultatas + IP_reikšmė_komandos_vykdymo_metu</td></tr>
<tr><td>Vidinis tiesioginis</td><td colspan="2">1. Iš mašininio kodo po OPK imamas 2 baitų poslinkis.
2. Baitai sukeičiami vietomis.
3. IP:= gautas_rezultatas + IP_reikšmė_komandos_vykdymo_metu</td></tr>
<tr><td>Išorinis tiesioginis</td><td colspan="2">1. Iš mašininio kodo po OPK imami 4 baitai.
2. Jie priskiriami CS ir IP registrams tokiu eiliškumu: IP j.b., IP v.b, CS j.b., CS v.b.
Pvz.: EA 11 22 33 44. IP=2211, CS=4433.</td></tr>
<tr><td rowspan="2">Vidinis netiesioginis</td><td colspan="2">Analizuojamas adresavimo baitas (reg dalis yra OPK plėtinys)</td></tr>
<tr><td>Mod=11 → IP registrui priskiriama žodinio registro reikšmė, kurią nurodo r/m.</td><td>Mod!=11 → einama į atminties vietą, kurią rodo operandas (mod ir r/m) ir paimami 2 baitai (IP j.b., IP v.b.), kurie tampa nauja IP reikšme.</td></tr>
<tr><td rowspan="2">Išorinis netiesioginis</td><td colspan="2">Analizuojamas adresavimo baitas (reg dalis yra OPK plėtinys)</td></tr>
<tr><td>Mod negali būti 11!</td><td>Einama į atminties vietą, kurią rodo operandas atmintyje (mod ir r/m) ir paimami 4 baitai eiliškumu IP j.b., IP v.b., CS j.b., CS v.b.</td></tr>
</table>

Sąlyginis valdymo perdavimas (1)

Visi atvejai (LOOP, sąlyginiai JMP) išskyrus INTO: komanda užima 2 baitus. 1-as baitas – OPK, 2-as baitas – poslinkis.

- INTO – vykdo INT 4, jeigu OF = 1 (OPK = CE, visa komanda – 1 baitas).
  1. Ar OF = 1?
  2. Taip → vykdoma INT 4.
     Ne → vykdomas sekanti komanda, kode esanti po INTO
- LOOP atvejai:
  1. CX:=CX-1 (VISADA);
  2. Ar tenkinama sąlyga?
  3. Taip → šokama su vieno baito poslinkiu (IP:=IP_komandos_vykdymo_metu + poslinkis (išplėstas pagal ženklą))
     Ne → vykdoma sekanti komanda, kode einanti po nagrinėto LOOP atvejo

Sąlyginis valdymo perdavimas (2)

- Sąlyginiai JMP atvejai (JO, JNO, JAE, JZ, JBE ir t.t.):
  1. Ar tenkinama sąlyga?
  2. Taip → šokama su vieno baito poslinkiu (IP:=IP_komandos_vykdymo_metu + poslinkis (išplėstas pagal ženklą))
     Ne → vykdoma sekanti komanda, kode einanti po sąlyginio JMP

Komandų operacijų kodai

Reikia mokėti:

1. JMP
2. CALL
3. RET
4. IRET

Nebūtina mokėti:

1. Sąlyginiai JMP
2. LOOP atvejai
3. INT atvejai

Operacijų kodus galima rasti dėstytojo konspekte, Beno konspekte bei dėstytojo Andrikonio sudarytame sąraše.

Pavyzdinis uždavinys (1)

Registrų reikšmės yra: DS=21FE, SS=5634, CS=0ADF, ES=41E3, BP=9A32, BX=7100, SI=0011, DI=22F1. Koks bus procedūros išorinio iškvietimo absoliutus adresas:

9715 2E FF 9F 16 26 call cs: number (9715– poslinkis kodo segmente)

- Tikslas – rasti procedūros iškvietimo absoliutų adresą
- Sąlygoj duota, kad vyksta CALL. Kadangi OPK – FF ir plėtinys yra 011, tai išorinis netiesioginis CALL.
- Vadinasi, vyksta besąlyginis **išorinis netiesioginis** valdymo perdavimas – absoliutus adresas suformuojamas paėmus 4 baitus iš atminties.

Pavyzdinis uždavinys (2)

1. Analizuojam adresavimo baitą. 9F = 10 011 111.
2. Mod = 10 → poslinkis 2 baitų.
3. R/m=111 → operando efektyvus adresas formuojamas taip: BX + 2 baitų poslinkis.
4. EA= 7100 + 2616 = 9716h

- Naudotas prefiksas 2E → vadinasi, operando atmintyje absoliutaus adreso formavimui naudojamas CS.
- Gavome, kad iš atminties vietos CS:9716 reikia paimti 4 baitus ir formuoti naujus IP ir CS (nes tai **išorinis netiesioginis** atvejis)
- Kokį atminties gabalą mes turim?

Pavyzdinis uždavinys (3)

- Prisimenam sąlygą:
  9715 2E FF 9F 15 26 call cs: number (9715– poslinkis kodo segmente)
- Vadinasi, duotas atminties gabalas iš kodo segmento su poslinkiu 9715. Reiškia, mūsų ieškomi baitai iš atminties su adresu CS:9716 yra matomi sąlygoje.
- Imam 4 baitus nuo CS:9716 reikiama tvarka:
  FF – IP j.b.
  9F – IP v.b.
  15 – CS j.b.
  26 – CS v.b.
- Turim, kad CS=2615, IP=9FFF. Formuojam absoliutų adresą pagal formulę AA=seg_reg_reikšmė * 10h + EA.
- Procedūros iškvietimas yra formuojamas pagal CS ir IP, vadinasi, AA=CS*10h+IP
- AA = 2615*10+9FFF = 3014F.

Ats.: 3014Fh.

Uždaviniai

1. AL=03, BL=02, CL=00, DL=01, AH=00, BH=01, CH=02, DH=03, ES=0000, CS=ABCD, SS=1234, DS=FE21, SP=2222, SF=0000. Įvykdžius nurodytą komandą, apskaičiuoti registrų reikšmių sumą: AL + BL + CL + DL + IP
   0100 E2 90 90 LOOP… (0100 yra poslinkis kodo segmente)
2. AX=0003, BX=0002, CX=0000, DX=0001. Įvykdžius nurodytą komandą, apskaičiuoti sekančios vykdomos komandos efektyvų adresą.
   FFFE EB FE JMP number (FFFE yra poslinkis kodo segmente)
3. DS=1111, ES=2222, CS=FFFF, SS=4444. Koks bus sekančios komandos absoliutus adresas, jei ta komanda bus vykdoma kodo segmente.
   0F01 E8 FF 00 CALL mom (0F01 yra poslinkis kodo segmente)
4. AL=01, BL=02, CL=03, DL=04, AH=52, BH=63, CH=74, DH=FF. Koks bus sekančios komandos efektyvus adresas, jei vykdoma komanda:
   FAAF FF E2 AA BB JMP places (FAAF yra poslinkis kodo segmente)

Uždavinių atsakymai

1. 197h
2. FFFEh
3. 00FF3h
4. FF04h