

Šeštoji paskaita

Stekas. Valdymo perdavimo būdai

Julius Andrikonis
julius.andrikonis@mif.vu.lt
Matematikos ir informatikos fakultetas
Vilniaus universitetas

Stekas

- SS:SP rodo į paskutinį užpildytą steko elementą;
- PUSH operandas:
 - $SP := SP - 2$
 - $[SS:SP] := \text{operandas}$
- POP operandas:
 - $\text{operandas} := [SS:SP]$
 - $SP := SP + 2$

Besąlyginio valdymo perdavimo komanda JMP (1)

- Vidinis artimas valdymo perdavimas:
 - 1110 1011 poslinkis
 - poslinkis – 1 baido skaičius su ženklų
 - $IP := IP + \text{poslinkis}$
 - poslinkis plečiamas iki dviejų baidų pagal skaičių su ženklų plėtimo taisyklę
- Vidinis tiesioginis valdymo perdavimas:
 - 1110 1001 posl.j.b posl.v.b
 - poslinkis – 2 baidų skaičius su ženklų
 - $IP := IP + \text{poslinkis}$

Besąlyginio valdymo perdavimo komanda JMP (2)

- Išorinis tiesioginis valdymo perdavimas:
 - 1110 1010 adr.j.b adr.v.b seg.j.b. seg.v.b
 - CS:= segmentas
 - IP:= adresas
- Vidinis netiesioginis valdymo perdavimas:
 - 1111 1111 mod 100 r/m [poslinkis]
 - Pagal mod, r/m ir poslinkį apskaičiuojamas operandas
 - IP:= operandas

Besąlyginio valdymo perdavimo komanda JMP (3)

- Išorinis netiesioginis valdymo perdavimas:
 - $1111\ 1111 \bmod 101\ r/m$ [poslinkis]
 - mod negali būti 11
 - pagal mod, r/m ir poslinkį apskaičiuojamas adresas;
 - $IP := [\text{adresas}]$
 - $CS := [\text{adresas} + 2]$

1 Uždavinys su JMP

- CS= 1234. Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: EB EC (0014 – poslinkis kodo segmente)

- EB= 1110 1011 => Vidinis artimas JMP => komanda užima 2 baitus
- IP komandos vykdymo metu visada rodo į kitą komandą, taigi IP= 0014+2= 0016;
- Po komandos IP= 0016+FFEC= 0002
- ea:= 0002
- aa:= 12340+0002= 12342

2 Uždavinys su JMP

- CS= 1234. Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: E9 F9 FF (0014 – poslinkis kodo segmente)

- E9= 1110 1001 => Vidinis tiesioginis JMP => komanda užima 3 baitus
- Komandos vykdymo metu IP= 0014+3= 0017;
- Po komandos IP= 0017+FFF9= 0010
- ea:= 0010
- aa:= 12340+0010= 12350

3 Uždavinys su JMP

- CS= 1234. Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: EA 12 FF 25 91 (0014 – poslinkis kodo segmente)

- EA= 1110 1010 => Išorinis tiesioginis JMP
- IP:= FF12
- CS:= 9125
- ea:= FF12
- aa:= 91250+FF12= A1162

4 Uždavinys su JMP (1)

- CS= 1234, BX= 0008. Duomenų segmento pirmieji 16 baitų atrodo taip:

0000: 00 01 02 03 04 05 06 07

0008: 08 09 0A 0B 0C 0D 0E 0F

Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: FF 67 05 (0014 – poslinkis kodo segmente)

- FF = 1111 1111, 67 = 01 100 111 => Vidinis netiesioginis JMP

4 Uždavinys su JMP (2)

- $\text{mod} = 01 \Rightarrow$ poslinkis 1 baito
- $\text{r/m} = 111 \Rightarrow \text{BX} + \text{poslinkis}$
- Poslinkis: 05 $\Rightarrow 5$
- Adresas duomenų segmente: $\text{BX} + 5 = 000\text{D}$
- $\text{IP} := \text{DS}:[000\text{D}] = 0\text{E}0\text{D}$
- $\text{ea} = 0\text{E}0\text{D}$
- $\text{aa} = 12340 + 0\text{E}0\text{D} = 1314\text{D}$

5 Uždavinys su JMP (1)

- CS= 1234, BX= 0008. Duomenų segmento pirmieji 16 baitų atrodo taip:

0000: 00 01 02 03 04 05 06 07

0008: 08 09 0A 0B 0C 0D 0E 0F

Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: FF E3 (0014 – poslinkis kodo segmente)

- FF = 1111 1111, E3 = 11 100 011 => Vidinis netiesioginis JMP

5 Uždavinys su JMP (2)

- $\text{mod} = 11 \Rightarrow$ lauke r/m – registras
- $\text{r/m} = 011 \Rightarrow \text{BX}$
- $\text{IP} := \text{BX} = 0008$
- $\text{ea} = 0008$
- $\text{aa} = 12340 + 0008 = 12348$

6 Uždavinys su JMP (1)

- CS= 1234, BX= 0008, SI= 0001. Duomenų segmento pirmieji 16 baitų atrodo taip:

0000: 00 01 02 03 04 05 06 07

0008: 08 09 0A 0B 0C 0D 0E 0F

Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

0014: FF 68 FD (0014 – poslinkis kodo segmente)

- FF = 1111 1111, 68 = 01 101 000 => Išorinis netiesioginis JMP

6 Uždavinys su JMP (2)

- $\text{mod} = 01 \Rightarrow$ poslinkis 1 baito
- $\text{r/m} = 000 \Rightarrow \text{BX} + \text{SI} + \text{poslinkis}$
- Poslinkis: FD \Rightarrow FFFD = -3
- Adresas duomenų segmente: $\text{BX} + \text{SI} - 3 = 0006$
- $\text{IP} := \text{DS}:[0006] = 0706$
- $\text{CS} := \text{DS}:[0006+2] = \text{DS}:[0008] = 0908$
- $\text{ea} = 0706$
- $\text{aa} = 09080 + 0706 = 09786$

Sąlyginio valdymo perdavimo komandos

- Sąlyginio valdymo komandos turi tik vidinį artimą variantą:
 - Komanda poslinkis
 - poslinkis – 1 baido skaičius su ženklų
- Sąlyginio valdymo komandų OPK:

JA, JNBE	77	JG, JNLE	7F	JO	70
JAE, JNB, JNC	73	JGE, JNL	7D	JNO	71
JNAE, JB, JC	72	JNGE, JL	7C	JP, JPE	7A
JNA, JBE	76	JNG, JLE	7E	JNP, JPO	7B
JZ, JE	74	JS	78	JCXZ	E3
JNZ, JNE	75	JNS	79		

Ciklo komandos

- Ciklo komandos turi tik vidinį artimą variantą:
 - Komanda poslinkis
 - poslinkis – 1 baido skaičių su ženklū
- Ciklo komandų OPK:
 - LOOP: E2 poslinkis
 - LOOPE, LOOPZ: E1 poslinkis
 - LOOPNE, LOOPNZ: E0 poslinkis

Paprogramēs iškviatimo komanda CALL (1)

- Vidinis tiesioginis:
 - 1110 1000 posl.j.b posl.v.b
 - Veiksmi:
 - PUSH IP
 - $IP := IP + \text{poslinkis}$
- Išorinis tiesioginis:
 - 1001 1010 adr.j.b. adr.v.b seg.j.b seg.v.b
 - Veiksmi:
 - PUSH CS
 - PUSH IP
 - $CS := \text{segmentas}$
 - $IP := \text{adresas}$

Paprogramēs iškviatimo komanda CALL (2)

- Vidinis netiesioginis:
 - 1111 1111 mod 010 r/m posl.j.b [posl.v.b]
 - Veiksmi:
 - PUSH IP
 - IP:= operandas
- Išorinis netiesioginis:
 - 1111 1111 mod 011 r/m posl.j.b [posl.v.b]
 - Veiksmi:
 - PUSH CS
 - PUSH IP
 - IP:= [adresas]
 - CS:= [adresas+2]

Grįžimo iš paprogramės komanda RET (1)

- Vidinė be steko išlyginimo:
 - 1100 0011
 - Veiksmai:
 - POP IP
- Vidinė su steko išlyginimu:
 - 1100 0010 bet.op.j.b bet.op.v.b
 - Veiksmai:
 - POP IP
 - $SP := SP + \text{betarpiškas operandas}$

Grįžimo iš paprograminės komanda RET (2)

- Išorinė be steko išlyginimo:
 - 1100 1011
 - Veiksmai:
 - POP IP
 - POP CS
- Išorinė su steko išlyginimu:
 - 1100 1010 bet.op.j.b bet.op.v.b
 - Veiksmai:
 - POP IP
 - POP CS
 - $SP := SP + \text{betarpiškas operandas}$

Pertraukimo iškvietimo komanda INT

- 1100 1101 tipas
- tipas – 1 baito
- Veiksmai:
 - PUSH SF
 - PUSH CS
 - PUSH IP
 - IF:= 0
 - TF:= 0
 - IP:= 0000:[tipas*4]
 - CS:= 0000:[tipas*4 + 2]

Komandos INT variantai

- INT 3 turi atskirą mašininį kodą 1100 1100
- Komanda INTO
 - Mašininis kodas 1100 1110
 - Jeigu OF=1, vykdoma komanda INT 4
- Klaidos atitaisymas: jei TF=1, tai po kiekvienos komandos įvyksta pertraukimas su numeriu 1 (o ne 4)!

Grijžimo iš pertraukimo komanda IRET

- 1100 1111
- Veiksmai:
 - POP IP
 - POP CS
 - POP SF