JUMP ir CALL

SS KA 2015-11-10 Miglė

Valdymo perdavimas

Sąlyginis

Besąlyginis

IP registro reikšmė

Nuolatos rodo į sekančią komandą

Reikia žinoti kiek baitų užima programa

Arba reikia suskaičiuoti

Perdavimo tipai

Vidinis artimas

Vidinis tiesioginis

Išorinis tiesioginis

Vidinis netiesioginis

Išorinis neteisioginis

Tipas	CALL	JUMP
Vidinis artimas	-	EB
Vidinis tiesioginis	E8	E9
Išorinis tiesioginis	9A	EA
Vidinis netiesioginis	FF *010	FF *100
Išorinis netiesioginis	FF *011	FF *101

*OPK plėtinys

**CALL atveju PUSH CS PUSH IP

RET

Grįžimas iš CALL

POP IP, POP CS

Reikalingas steko išlyginimas SP:=SP+bet.op

RET tipas	Su steko išlyginimu	Be steko išlyginimo
Vidinis	C2	C3
Išorinis	CA	CB

INT n, IRET

PUSH SF, PUSH CS, PUSH IP, IF=0, TF=0, AA 4n imami 4 baitai;

POP IP, POP CS, POP SF;

IRET kodas CF

Sąlyginis valdymo perdavimas

INTO

LOOP

17 JMP

INTO

INT 4, jeigu flagas OF=1.

Operacijos kodas CE.

LOOP

Veiksmai

-sumažinti CX 1;

-tikrinti sąlygą, jei tenkinama, pridėti 1B;

Komanda	Peršokimui su vieno baito poslinkiu būtina sąlyga
LOOP	gautas CX nelygus 0000
LOOPE LOOPZ	gautas CX nelygus 0000 IR flagas ZF=1
LOOPNE LOOPNZ	gautas CX nelygus 0000 IR flagas ZF=0

JMP if

KOMANDOS PAVADINIMAS	PAVADINIMO PRASMĖ	TIKRINAMA SĄLYGA
JO	Jump if Overflow	OF=1
JNO	Jump if Not Overflow	OF=0
JNAE JB JC	Jump if Not Above nor Equal Jump if Below Jump if Carry	CF=1
JAE JNB JNC	Jump if Above or Equal Jump if Not Below Jump if Not Carry	CF=0

JE JZ	Jump if Equal Jump if Zero	ZF=1
JNE JNZ	Jump if Not Equal Jump if Not Zero	ZF=0
JBE JNA	Jump if Below or Equal Jump if Not Above	CF=1 ARBA ZF=1 (bent vienas)
JA JNBE	Jump if Above Jump if Not Below nor Equal	CF=0 IR ZF=0 (reikalingi abu)
JS	Jump if Sign	SF=1
JNS	Jump if Not Sign	SF=0
JP JPE	Jump if Parity Jump if Parity Equal	PF=1
JNP JPO	Jump if Not Parity Jump if Parity Odd	PF=0

JL JNGE	Jump if Lower Jump if Not Greater nor Equal	SF nelygu OF
JGE JNL	Jump if Greater or Equal Jump if Not Lower	SF=OF
JLE JNG	Jump if Lower Or Equal Jump if Not Greater	ZF=1 arba (SF nelygu OF) (bent vienas)
JG JNLE	Jump if Greater Jump if Not Lower nor Equal	ZF=0 ir SF=OF (reikalingi abu)
JCXZ	Jump if CX Zero	CX=0

0111 0000 poslinkis – JO žymė

0111 0001 poslinkis – JNO žymė

0111 0010 poslinkis – JNAE žymė; JB žymė; JC žymė

0111 0011 poslinkis – JAE žymė; JNB žymė; JNC žymė

0111 0100 poslinkis – JE žymė; JZ žymė

0111 0101 poslinkis – JNE žymė; JNZ žymė

0111 0110 poslinkis – JBE žymė; JNA žymė

0111 0111 poslinkis – JA žymė; JNBE žymė

0111 1000 poslinkis – JS žymė

0111 1001 poslinkis – JNS žymė

0111 1010 poslinkis – JP žymė; JPE žymė

0111 1011 poslinkis – JNP žymė; JPO žymė

0111 1100 poslinkis – JL žymė; JNGE žymė

0111 1101 poslinkis – JGE žymė; JNL žymė

0111 1110 poslinkis – JLE žymė; JNG žymė

0111 1111 poslinkis – JG žymė; JNLE žymė

Sutrumpinimas

J raidė reiškia žodį Jump

N – not, nor. O – odd. Sąlygos paneigimas.

C,Z,S,P – reiškia atitinkamus flagus

A – above (skaičiuose be ženklo), G – greater (skaičiuose su ženklu) reiškia „daugiau“

B – below (skaičiuose be ženklo), L – lower (skaičiuose su ženklu) reiškia „mažiau“

E – equal – lygu

JO, JNO atveju O raidė reiškia OF flagą

1 PS2013

Įvykdžius nurodytą komandą, apskaičiuoti registrų reikšmių sumą:
AL+BL+CL+DL+IP, kai 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:
0100 E2 90 90 loop ... (0100 yra poslinkis kodo segmente)

2. IT2013

2. Įvykdžius nurodytą komandą, apskaičiuoti sekančios vykdomos komandos absoliutų adresą, kai DS=21FE, SS=5634, CS=0ADF, ES=41E3, BP=9A32, SI=FFF1, DI=22F1, AX=0003, BX=0002, CX=0000, DX=0001, SF=0000:
DCBA E0 90 90 loopne ... (DCBA yra poslinkis kodo segmente)

3. IT2013

6. Registrų reikšmės yra: SI=FFF0, DS=1234, DI=FFFF, ES=1233, registras CX=FFFF, registras SF=FF00.
Kokia bus steko viršūnės reikšmė įvykdžius procedūros tolimo iškvietimo komandą:
46DE 2E FF 59 F9 37 90 90 call cs:... (46DE yra poslinkis kodo segmente)

4.

1. CS=FFFF
9999: 9A 12 34 56 78
Koks yra kviečiamos procedūros AA?

5.

2. CS=ABCD, SS=7894, DS=2222, ES=3333, SP=0001 SI=1111 DI=7894 BP=92A2, BX=BEBE
Vykdomas kodas:
1234: 2E FF D4 90 90 90
1) Sekančios komandos AA?
2) Kviečiamos procedūros AA?

6.

Turimos registrų reikšmės yra AX=7897, BX=AA2E, CX=EE32, DX=12EE, SI=AAEE, DI=DDAA, CS=78AA, SS=DEAE, DS=7700, ES=2EAA.
Apskaičiuokite sekančios vykdomos komandos absoliutų adresą, jei vykdoma komanda...:
9090: E9 90 90 90 90 90 90 90 90 90 (9090 – poslinkis kodo segmente)

7

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

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

8

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

```
0000: 80 81 82 83 84 85 86 87
0008: 88 89 8A 8B 8C 8D 8E 8F
```

Apskaičiuokite kitos vykdomos komandos ea ir aa, įvykdžius komandą:

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

9.

3. Registrų reikšmės yra: DS=FE21, SS=3456, CS=C131, ES=3EE3, BP=92A2, BX=C5D6, SI=45FA, DI=22F1, SP=FFF6. Kokia bus registro SP reikšmė, įvykdžius grįžimo iš artimos procedūros komandą:

C2 10 00

Atsakymai

1. 197
2. 18A3C
3. 46E2
4. 7B792
5. B4F72
6. 7ABC3
7. EA= 0010; AA=12350
8. EA=8E8D AA=1B1CD
9. 0008