ASEMBLER – kontrolne strukture

1. Kontrolne strukture

Jezici visokog nivoa sadrže strukture za kontrolu toka koje su takođe visokog nivoa, npr. *if* i *while* sa preduslovom i postuslovom. Asembler ne omogućava tako "kompleksne" strukture. Umesto toga, koristi se nepopularni *goto* za čitavu kontrolu toka programa.

Ako se *goto* koristi na neodgovarajući način, svaki program (pa i asemblerski) postaje nečitak i težak za održavanje. Uprkos tome, korišćenjem pravila strukturiranog programiranja, može se postići da čak i asemblerski kod bude strukturiran.

2. Poređenja

Kontrolne strukture odlučuju šta da rade bazirajući se na poređenju podataka. U asembleru, rezultat tog poređenja se čuva u FLAGS registru. 80x86 procesori koriste CMP instrukciju za izvođenje poređenja, dok se FLAGS registar menja u skladu sa rezultatom. CMP instrukcija je, u stvari, SUB (oduzimanje drugog od prvog operanda) , s tim što se rezultat oduzimanja nigde ne čuva.

Za neoznačene cele brojeve, dve zastavice (bita u FLAGS registru) su bitne, i to: ZF (*zero flag* - nula) i CF (*carry flag* - prenos). ZF se postavlja na 1 ako je rezultat operacije razlike 0. CF se u operaciji razlike koristi kada dođe do "pozajmice". Na primer:

```
cmp vleft, vright
```

Dakle, izračunava se razlika vleft - vright i FLAGS registar se postavlja prema rezultatu. Ako je razlika 0, tj. vleft=vright, tada se ZF postavlja na 1, dok je CF nula (nema pozajmice). Ako je vleft>vright, i ZF i CF su nule. Ako je vleft<vright, tada je ZF=0, a CF=1 (došlo je do pozajmice).

Ne treba zaboraviti da i druge instrukcije menjaju FLAGS registar, a ne samo CMP! Poređenje označenih brojeva je nešto komplikovanije, pa na ovom mestu neće biti diskutovano.

3. Instrukcije grananja

Instrukcije grananja služe za transfer izvršavanja na bilo koju tačku unutar programa. Drugim rečima, ove instrukcije igraju ulogu kao *goto* u nekim programskim jezicima. Postoje dve vrste ovih instrukcija - uslovne i bezuslovne. Bezuslovna instrukcija je baš kao *goto*, do skoka dolazi uvek. Uslovne instrukcije grananja mogu, ali ne moraju da izvrše grananje, zavisno od stanja FLAGS registra. Ako do grananja ne dođe, kontrola se daje prvoj sledećoj instrukciji.

Instrukcija bezuslovnog skoka je JMP. Njen jedini argument je *labela* instrukcije na koju se skače. Labelu asembler i linker zamenjuju konkretnom memorijskom adresom. Važno je napomenuti da instrukcija odmah posle JMP neće biti nikad izvršena, osim ako se neka druga instrukcija grana na nju.

Validne labele u kodnom segmentu (*.text*) se definišu svojim nazivom i dvotačkom, nakon čega sledi instrukcija, kao npr:

```
while_granica:      mov     eax,[broj]
```

Neke od instrukcija uslovnog grananja date su u sledećoj tabeli. Kao svoj operand sve one uzimaju labelu, kao i JMP.

JZ	skok ako je ZF=1, zero, nula
JNZ	skok ako je ZF=0
JO	skok ako je OF=1, overflow, izlaz iz opsega
JNO	skok ako je OF=0
JS	skok ako je SF=1, sign, znak
JNS	skok ako je SF=0
JC	skok ako je CF=1, carry, prenos
JNC	skok ako je CF=0
JP	skok ako je PF=1, parity, parnost nižih 8 bita
JNP	skok ako je PF=0

Sledeći C-ovski pseudo kod:

```
if ( EAX == 0 )
      EBX = 1;
else
      EBX = 2;
```

u asembleru može da se napiše kao:

```
      cmp eax, 0              ; postavljanje zastavica (ZF=1 ako eax-0=0)
      jz then_blok            ; ako je ZF setovan, skoci na then_blok
      mov ebx, 2              ; ELSE deo IF-a
      jmp next                ; preskoci THEN deo
then_blok:
      mov ebx, 1              ; THEN deo IF-a
next:
```

Međutim, ostala poređenja, npr. <=, >= nije tako lako izvesti koristeći samo instrukcije iz tabele. Problem je što mora da se vodi računa o nekoliko zastavica istovremeno.

Na sreću, procesori tipa 80x86 poseduju instrukcije koje omogućavaju mnogo korisnički orijentisanije grananje. Te instrukcije, i to samo za neoznačne cele brojeve kao operande date su u sledećoj tabeli:

JE	skače ako vleft = vright
JNE	skače ako vleft != vright
JB, JNAE	skače ako vleft < vright
JBE, JNA	skače ako vleft <= vright
JA, JNBE	skače ako vleft > vright
JAE, JNB	skače ako vleft >= vright

Recimo, JB i JNAE su instrukcije sinonimi jer je:

$$x < y \Leftrightarrow \textbf{not}\,(x \geq y)$$

Evo kako bi se u asembler preveo sledeći C kod:

```
// C kod
if ( EAX >= 5 )
      EBX = 1;
else
      EBX = 2;

; asemblerski kod
      cmp eax, 5
      jae then_blok
```

```
      mov ebx, 2
      jmp next
then_blok:
      mov ebx, 1
next:
```

4. Prevođenje standardnih kontrolnih struktura

Ova sekcija data je kao pomoć programeru kod prevođenja standardnih struktura kontrole toka iz viših programskih jezika u asemblerski kod.

4.1 If klauzule

Sledeći pseudo kod:

```
if ( uslov )
      then blok ;
else
      else blok ;
```

može se implementirati ovako:

```
      ; kod za setovanje FLAG zastavica
      jxx   else_blok   ; jxx se postavlja tako da je if uslov false!
      ; kod then bloka
      jmp endif

else_blok:
      ; kod else bloka
endif:
```

U slučaju da nema *else* bloka, instrukcija uslovnog grananja skače na endif:

```
      ; kod za setovanje FLAG zastavica
      jxx   endif       ; jxx se postavlja tako da je if uslov false!
      ; kod then bloka
endif:
```

4.2 While petlje

Opšta forma *while* petlje je:

```
while ( uslov ) {
      telo petlje;
}
```

što se u asembleru implementira ovako:

```
while:
      ; kod za setovanje FLAG zastavica
      jxx endwhile      ; izabrati xx tako da je uslov==false
      ; telo petlje
      jmp while
endwhile:
```

4.3 Do-while petlje

Kod *do-while* petlje uslov se testira na kraju:

```
do {
      telo petlje;
```

```
} while ( uslov );
```

što u prevedenom obliku daje:

```
do:
      ; telo petlje
      ; kod za setovanje FLAG zastavica
      jxx do      ; izabrati xx tako da je uslov==true
```

4.4 For petlje

80x86 poseduje nekoliko instrukcija za implementaciju for petlji. Najpoznatija je instrukcija LOOP koja za brojač korsiti ECX registar koji dekrementira, pa ako je ECX!=0 skače na labelu koja se navodi kao argument.

Sledeći pseudo kod:

```
suma = 0;
for ( i =10; i >0; i -- )
      suma += i;
```

bi se u asembler preveo ovako:

```
      mov eax,0         ; eax je suma
      mov ecx, 10       ; ecx je i
loop_start:
      add eax, ecx
      loop loop_start
```

Deljenje

Instrukcija DIV je instrukcija celobrojnog deljenja. Deljenik se smešta u kombinaciju registara EDX:EAX (64 bita ukupno), nakon čega se deli operandom instrukcije DIV. Rezultat se smešta u EAX, dok se ostatak u EDX.

Množenje

Slično tome, celobrojno množenje 32-bitnih celobrojnih vredosti se obavlja instrukcijom

```
mul source
```

gde se 32-bitna vrednost na koju pokazuje *source* množi sadržajem registra EAX, a 64-bitni rezultat se smešta u kombinaciju registara EDX:EAX.