Kaip parašyti asm3

t. y. Kaip parašyti trečiąją programą asembleriu

Programos rašymo tikslai:

1. Suprasti kaip veikia pertraukimų mechanizmas
2. Parašyti savo pertraukimą apdorojančią procedūrą
3. Mokėti programiškai versti mašininį kodą į asemblerinį užrašą

Jums reikės suprogramuoti kažkurią iš pertraukimo apdorojimo procedūrų:
INT 0 – Dalybos iš nulio pertraukimas
INT 1 – Žingsninis pertraukimas
INT 3 – Kontrolinio taško pertraukimas
INT 4 – Perpildymo (overflow) pertraukimas

Kada jos vykdomos?

INT 0 – Įvyksta, kai dalinama iš nulio arba dalybos rezultatas netelpa į žodį arba baitą. Tarkim vieno baito dalybos komanda DIV bl daliname AX=1000h, BL=02h (rezultatas 800h netelpa viename baite)

INT 1 – Vyksta po kiekvienos komandos, kai SF registre požymis TF (Trap Flag) yra vienetas

INT 3 – Kontrolinio taško pertraukimas įvyksta ten kur kviečiamas komanda **INT 3**

INT 4 – Perpildymo pertraukimas įvyksta ten kur kviečiamas komanda INTO (įvyksta, jei flagas OF=1). Galbūt įvyksta ir po kokios nors komandos, kur OF yra nustatomas vienetu (reiktų tai patikrinti)

Kaip perimti pertraukimą?

Kad vykdytų ne numatytąjį programoje, o jūsų parašytą pertraukimą reikia vektorių lentelėje esantį pertraukimo apdorojimo procedūros adresą perrašyti savuoju.

INT n – komandos apdorojimo adresas yra absoliučiu adresu 4n. Nusistatome ES (ekstra segmento t.y. papildomo duomenų segmento registro) reikšmę, kad rodytų į vektorių lentelės pradžią. Į ES įrašome nulį. Kadangi nėra būdo įrašyti konstantą į segmentinį regsitrą, tai darome panaudodami kitą registrą (tarkim ax):
MOV ax, 0
MOV es, ax

Kai ES jau rodo į vektorių lentelės, tuo pačiu ir pačios atminties (RAM'ų) pradžią, einame su poslinkiu 4n ir pasiimame 2 žodžius. Pirmiau IP žodį, tada CS žodį. (žodis=2baitai, pirmiau jaunenysis, po to vyresnysis)

Pavyzdžiui domina žingsninis pertraukimas ***INT 1***. n=1.
Reiškia IP reikšmė yra adresu ES:0004
CS reikšmė yra adresu ES:0006

00004: IP jaunesnysis
00005: IP vyresnysis
00006: CS jaunesnysis
00007: CS vyresnysis

Pastaba: prieš perimant pertraukimą būtina išsisaugoti senas IP ir CS reikšmes, o kai pertraukimas mums nebereikalingas jas atstatyti!

Kaip aktyvuoti žingsninį rėžimą (reikia tik INT 1 atveju)

Norėdami, kad po kiekvienos komandos testiniame bloke būtų iškviestas žingsninis (po kiekvieno programos žingsnio) pertraukimas turite aktyvuoti Trap Flagą. (TF požymį SF registre nustatyti vienetu).

Kadangi nėra komandos darbui su TF ir jis nekinta vykdant aritmetines/logines komandas, tai teks tiesiogiai redaguoti SF reikšmę.

Nėra būdo prieiti prie SF reikšmės kitaip kaip per steką, vadinasi teks:

- Pasidėti SF į steką (PUSHF)
- Išsitraukti iš steko jo reikšmę į kokį nors darbinį registrą
- Nustatyti TF bitą vienetu (8tas iš kairės bitas) – pvz. panaudojant loginę komandą OR
- Padėti naują SF reikšmę į steką
- Steke vėliausiai padėtą reikšmę išsiimti į SF registrą (POPF)

Iš ko turi susidėti asm3 programa?

- Visi reikalingi kintamieji ir pranešimai duomenų segmente
- Mov ax, @data ir MOV ds, ax eilutės
- Pagalbos parametro /? apdorojimas (jei reikalaujama)
- Išsisaugoti seną CS ir seną IP tos pertraukimo procedūros, kurią ketiname perrašyti savuoju pertraukimu
- Perimti pertraukimą
- Aktyvuoti žingsninį rėžimą (nustatyti flagą TF=1)
- Prirašyti kokių nors komandų testiniam bloke (čia rašomos bet kokios komandos, svarbiausia, kad būtų tokių, kurios iškviečia jūsų aprašytą pertraukimą)
- Išjungti žingsninį rėžimą
- Atstatyti seną pertraukimo adresą (CS,IP)
- Baigti programos darbą

- Pertraukimo apdorojimo procedūra:
  - Duomenų segmente išsisaugom iškviečiant pertraukimą esančias AX,BX,CX,DX,SP,BP,SI,DI reikšmes
  - Pasiimam CS,IP reikšmes iš steko (buvo įdėtos iškviečiant pertraukimą) tarkim į SI,DI
  - Pasiimt mašininio kodo baitus pradedant CS:nagrinėjamos_komandos_ip
  - Pasitikriname ar mokame atpažinti komandą, jei ne peršokame į pertraukimo procedūros užbaigimą
  - Jei sutikome segmento keitimo prefiksą išsisaugome informaciją apie tai duomenų segmente
  - Spausdiname CS,IP komandos ir baitus (įskaitant prefikso baitą)
  - Spausdiname visą kitą reikalingą komandos informaciją, pagal reikalavimus
  - Pertraukimo procedūros užbaigimas:
    - Iš duomenų segmento atstatome iškviečiant pertraukimą buvusias AX,BX,CX,DX,SP,BP,SI,DI reikšmes
    - komanda IRET atliekame grįžimą iš pertraukimo apdorojimo procedūros

- Toliau gali būti įvairių pagalbinių pertraukime reikalingų procedūrų kodai, tarkim šešioliktainių skaičių spausdinimo ir kitos.