Języki asemblerowe

WYKŁAD 3

Dr Krzysztof Balicki

Podstawowe rejestry procesora Pentium

- Osiem rejestrów ogólnego przeznaczenia
- Sześć rejestrów segmentowych
- Rejestr znaczników
- Wskaźnik (licznik) rozkazów

Rejestry ogólnego przeznaczenia

- 32-bitowe rejestry:
  - EAX – akumulator
  - EBX – rejestr bazowy
  - ECX – licznik pętli oraz operacji na łańcuchach
  - EDX – rejestr danych
  - EBP – wskaźnik bazowy
  - ESI – rejestr indeksowy źródła
  - EDI – rejestr indeksowy celu
  - ESP – wskaźnik stosu
- Powyższe rejestry mogą być używane w inny sposób niż wynika to z ich nazwy

Rejestry ogólnego przeznaczenia

- Młodsze 16 bitów rejestrów ogólnego przeznaczenia odpowiada rejestrom ogólnego przeznaczenia procesorów 8086 oraz Intel 286, dostępnym przez nazwy: AX, BX, CX, DX, BP, SI, DI, SP.
- Starsze bajty rejestrów AX, BX, CX, DX dostępne są poprzez nazwy: AH, BH, CH, DH, odpowiednio.
- Młodsze bajty rejestrów AX, BX, CX, DX dostępne są poprzez nazwy: AL, BL, CL, DL, odpowiednio.

Rejestry segmentowe

- 16-bitowe rejestry:
  - CS - segment programu
  - DS - segment danych
  - SS - segment stosu
  - ES - dodatkowy rejestr
  - FS - dodatkowy rejestr
  - GS - dodatkowy rejestr
- Wykorzystywane są do adresacji pamięci operacyjnej

Adresowanie pamięci

- Fizyczna pamięć podzielona jest na segmenty logiczne.

$$\text{Adres fizyczny} = \text{segment} * 16_{10} + \text{offset}$$

Rejestr znaczników

- 32-bitowy rejestr EFLAGS zawierający znaczniki (flagi). Wybrane flagi:
  - bit 0 - CF - przeniesienie/pożyczka
  - bit 2 - PF - parzystość (wynik operacji ma parzystą liczbę jedynek w mniej znaczącym bajcie)
  - bit 4 - AF - pomocnicze przeniesienie (z bitu 3 na 4)/pożyczka (z bitu 4 na 3) - używane przy kodzie BCD
  - bit 6 - ZF - znacznik zera
  - bit 7 - SF - znacznik znaku
  - bit 11 - OF - nadmiar (przepełnienie)

Wskaźnik (licznik) rozkazów

- 32-bitowy rejestr EIP
- Wskazuje adres względem początku segmentu programu, skąd pobierany będzie kolejny rozkaz

Wybrane rozkazy

- **Rozkazy przesłań**: MOV, XCHG
- **Rozkazy arytmetyczne**: INC, DEC, ADD, SUB, MUL, IMUL (mnożenie ze znakiem), DIV, IDIV (dzielenie ze znakiem)
- **Rozkazy porównań**: CMP

Wybrane rozkazy

- **Rozkazy skoków**: JMP, JE (jeśli równe), JG (jeśli większe), JL (jeśli mniejsze), JGE (jeśli większe lub równe), JLE (jeśli mniejsze lub równe), JNE (jeśli różne), JZ (jeśli zero), JNZ (jeśli nie zero), JC (jeśli przeniesienie), JNC (jeśli brak przeniesienia), JO (jeśli przepełnienie), JNO (jeśli brak przepełnienia)

Wybrane rozkazy

- **Rozkazy logiczne**: AND, OR, XOR, NOT
- **Rozkaz pętli**: LOOP (ECX zawiera licznik pętli, skok gdy ECX ≠ 0), LOOPZ (ECX zawiera licznik pętli, skok gdy ECX ≠ 0 i ZF=1), LOOPNZ (ECX zawiera licznik pętli, skok gdy ECX ≠ 0 i ZF=0)

Wybrane rozkazy

- **Rozkazy przesunięć**: SHL, SHR
- **Rozkazy rotacji**: ROL, ROR, RCL, RCR
- **Rozkazy operacji na stosie**: PUSH, POP

Adresowanie argumentów

- Argumenty rejestrowe – określany jest nazwą odpowiedniego rejestru:

  REJESTR

- Argumenty pamięciowe – do obliczania adresu używane są:
  - rejestry: **[REJESTR]**
  - nazwy symboliczne
  - stałe

  w różnej kombinacji.

Wykorzystanie podprogramów systemowych

- System operacyjny udostępnia m.in. zestaw funkcji do obsługi urządzeń we/wy.
- W systemie MS-DOS większość funkcji jest dostępna poprzez wywołanie przerwania 21h.
- Numer funkcji wpisywany jest do rejestru AH, argumenty funkcji wpisywane są do pozostałych rejestrów.

Wybrane funkcje przerwania 21h

- AH=01h – czytanie znaku z echem, przeczytany znak zwracany jest w AL
- AH=02h – wypisanie znaku z DL
- AH=08h – czytanie znaku bez echa, przeczytany znak zwracany jest w AL
- AH=09h - wypisanie łańcucha znaków, DS:DX zawierają adres początku łańcucha, łańcuch kończy się znakiem $
- AH=0Bh – sprawdzenie bufora klawiatury, zwracane wartości: AL=00h (bufor pusty), AL=FFh (są znaki w buforze)

Wybrane funkcje przerwania 21h

- AH=3Ch – utworzenie pliku
  - DS:DX zawierają adres do specyfikacji pliku (łańcuch znaków zakończony 0),
  - CX zawiera atrybuty pliku:
    - bit 0: tylko do odczytu
    - bit 1: ukryty
    - bit 2: systemowy
    - bit 3: etykieta woluminu
    - bit 4: katalog
    - bit 5: archiwalny
  - uchwyt pliku zwracany jest w AX (jeśli CF=0 - poprawne wykonanie), kody błędów zwracane są w AX (jeśli CF=1 - błąd w wykonaniu).

Wybrane funkcje przerwania 21h

- AH=3Dh – otwarcie pliku
  - DS:DX zawierają adres do specyfikacji pliku,
  - AL zawiera tryb otwarcia pliku:
    - bity 2 - 0 definiują tryb dostępu: 000 - tylko odczyt, 001 - tylko zapis, 010 - odczyt i zapis,
    - bity 6 - 4 definiują tryb dzielenia: 000 - tryb zgodny (wszystkie procesy mają pełny dostęp do pliku), 001 - tryb wyłączności (inne procesy nie mają dostępu do pliku), 010 - tryb „tylko do odczytu” (inne procesy mogą odczytywać plik), 011 - tryb „tylko do zapisu” (inne procesy mogą zapisywać plik),
  - uchwyt pliku zwracany jest w AX (jeśli CF=0 - poprawne wykonanie), kody błędów zwracane są w AX (jeśli CF=1 - błąd w wykonaniu).

Wybrane funkcje przerwania 21h

- AH=3Eh – zamknięcie pliku
  - BX zawiera uchwyt pliku,
  - jeśli CF=0 - poprawne wykonanie, kody błędów zwracane są w AX jeśli CF=1 - błąd w wykonaniu.

Wybrane funkcje przerwania 21h

- AH=3Fh – odczyt z pliku
  - BX zawiera uchwyt pliku,
  - CX zawiera liczbę bajtów do odczytania,
  - DS:DX zawierają adres do bufora dla odczytanych bajtów,
  - liczba odczytanych bajtów zwracana jest w AX (jeśli CF=0 - poprawne wykonanie), kody błędów zwracane są w AX (jeśli CF=1 - błąd w wykonaniu)

Wybrane funkcje przerwania 21h

- AH=40h – zapis do pliku
  - BX zawiera uchwyt pliku,
  - CX zawiera liczbę bajtów do zapisu,
  - DS:DX zawierają adres do bufora dla zapisywanych bajtów,
  - liczba zapisanych bajtów zwracana jest w AX (jeśli CF=0 - poprawne wykonanie), kody błędów zwracane są w AX (jeśli CF=1 - błąd w wykonaniu)

Wybrane funkcje przerwania 21h

- AH=41h – usunięcie pliku
  - DS:DX zawierają adres do specyfikacji pliku (łańcuch znaków zakończony 0),
  - jeśli CF=0 - poprawne wykonanie, kody błędów zwracane są w AX jeśli CF=1 - błąd w wykonaniu.

Wybrane funkcje przerwania 21h

- AH=42h – przesunięcie wskaźnika pliku
  - BX zawiera uchwyt pliku,
  - CX:DX zawierają wielkość przesunięcia (liczba 4-bajtowa),
  - AL zawiera rodzaj przesunięcia:
    - 0 - względem początku pliku, 1 - względem bieżącej pozycji wskaźnika, 2 - względem końca pliku (dla 1 i 2 wielkość przesunięcia podawana jest w kodzie U2)
  - nowa pozycja wskaźnika zwracana jest w DX:AX (jeśli CF=0 - poprawne wykonanie), kody błędów zwracane są w AX (jeśli CF=1 - błąd w wykonaniu).

Wybrane funkcje przerwania 21h

- AH=4Ch – zakończenie procesu, kod powrotu umieszczany jest w AL

Alokacja pamięci

- Dane inicjalizowane

  [zmienna] typ wartość_początkowa

np.:

litera DB 'a'

- Typ:
  - DB - 1 bajt
  - DW - słowo (2 bajty)
  - DD - podwójne słowo (4 bajty)
  - DQ - poczwórne słowo (8 bajtów)
  - DT - 10 bajtów

Alokacja pamięci

- Dane nieinicjalizowane

[zmienna] typ rozmiar

np.:

znaki RESB 10

- Typ:
  - RESB - 1 bajt
  - RESW - słowo (2 bajty)
  - RESD - podwójne słowo (4 bajty)
  - RESQ - poczwórne słowo (8 bajtów)
  - REST - 10 bajtów

Deklaracja stałej

nazwa EQU wyrażenie

np.:

a EQU 5

Procedury

- Wywołanie:

CALL nazwa_procedury

- Powrót z procedury:

RET

- Przekazywanie parametrów:
  - przez rejestry (zaleta: szybkość, wada: mała ilość parametrów)
  - przez stos

Podstawowa struktura programu

```
bits 16
org 100h
section .data
...
section .bss
...
section .text
...
...
...
```

Segment danych inicjalizowanych

Segment danych nieinicjalizowanych

Segment kodu