**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО**

**ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №2

Дисциплина: Архитектура вычислительных систем

по теме Разработка программ на ассемблере.

Структура команд процессора

Выполнил: ст. группы ВТ-32  
 Воскобойников И. С.

Проверил: Осипов.О.В

**Белгород 2020**

Цель работы: изучить структуру команд процессора, научиться составлять машинный код простейших команд.

**Задания для выполнения к работе**

1. Ознакомиться с теоретическим материалом главы 2 учебника В.И. Юрова «Assembler» “Программно-аппаратная архитектура IA-32 процессоров Intel”.

2. В соответствии с вариантом задания определить по символьному описанию команд их машинный код (для 5 команд), а также по машинному коду команд определить их символьное описание (для 2 машинных кодов).

**Вариант 3**

**Символьное описание команд на языке Assembler**:

3. OR DI, 11110001b

MOV DWORD PTR [EBX], 'L'

TEST AX, [EDI+4Fh]

ADC CL, AL

CMP [EDX\*4+ESI+7], ECX

**Машинные коды команд в 16 системе счисления:**

8B5E 01

8AC3

**Команда 1:**  OR DI, 11110001b

**регистр DI** (*Destination Index*) – является индексом назначения и применяется так же для строковых операций (обычно связан с регистром ES).

OR -Логическое включающее "ИЛИ" 11110001b

Код операции данной команды **OR** **КОП**=1011. Размер пересылаемых данных равен 4 байтам, значит **w**=1. Регистру DI соответствует поле **reg**=111. Число 11110001d кодируется следующими четырьмя байтами. 11110001d = 00F1 = 11110001b. Байты числа представляются в памяти в обратном порядке, поэтому в коде команды первым будет младший байт 11110001b =00F1. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 241 | | | |
| 1111 | 1 | 111 | 11110001 | 00000000 | 00000000 | 00000000 |
| FF | | | F1h | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 11111111b=FFh. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду OR DI, 241 можно сделать вывод, что ей соответствует машинный код   
**FFF10000000h**. Длина команды – 5 байт.

**Команда 2:**  MOV DWORD PTR [EBX], 'L'

Команда выполняет пересылку DWORD символа ‘**L**’ в регистр PTR. Первый операнд имеет регистровую адресацию, второй является непосредственным операндом. Код операции данной команды **MOV** **КОП**=1100. Размер пересылаемых данных равен байта, значит **w**=0. Регистру PTR соответствует поле **reg**=111.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 76 | | | |
| 1100 | 0 | 111 | 01001100 | 00000000 | 00000000 | 00000000 |
| C7 | | | 4Ch | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 11000111b=C7h. Непосредственный операнд кодируется следующими 1 байтами. Проанализировав команду OR DI, 241 можно сделать вывод, что ей соответствует машинный код   
**C74C000000h**. Длина команды – 5 байт.

**Команда 3:**  TEST AX, [EDI+4Fh]

**TEST** Выполняет операцию логического И между двумя операндами, устанавливает соответствующие флаги состояния процессора, но результат операции не записывается вместо операнда получателя данных

Код операции данной команды TEST **КОП**=0100. Размер пересылаемых данных равен 1 байтам, значит **w**=0. Регистру AX соответствует поле **reg**=111. Число 01001010d кодируется следующими четырьмя байтами. 01001010d = 4Аh = 01001010b.. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 74 | | | |
| 0100 | 0 | 111 | 01001010 | 00000000 | 00000000 | 00000000 |
| 4F | | | 4Аh | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 01000111b=4Fh. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду TEST AX, 74 можно сделать вывод, что ей соответствует машинный код   
**4F4A000000h**. Длина команды – 5 байт.

**Команда 4:**  ADC CL, AL

Инструкция ADC в Ассемблере выполняет сложение с переносом.

Код операции данной команды ADC **КОП**=1100. Размер пересылаемых данных равен 4 байтам, значит **w**=1. Регистру CL соответствует поле **reg**=000. Число 11001000d кодируется следующими четырьмя байтами. 11001000d = С8= 11001000d. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 8 | | | |
| 1100 | 1 | 000 | 00001000 | 00000000 | 00000000 | 00000000 |
| С8 | | | 08h | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 11001000d = С8. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду ADC CL, 8 можно сделать вывод, что ей соответствует машинный код   
**C808030000h**. Длина команды – 5 байт.

**Команда 5:**  CMP [EDX\*4+ESI+7], ECX

Команда CMP процессоров семейства i80x86 используется для сравнения двух операндов. Говоря проще, эта команда сравнивает два числа, то есть проверяет, равны эти два числа или НЕ равны.Код операции данной команды CMP **КОП**=1100. Размер пересылаемых данных равен 4 байтам, значит **w**=1. Регистру EDX\*4+ESI+7 соответствует поле **reg**=001. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 7 | | | |
| 1100 | 1 | 001 | 00000111 | 00000000 | 00000000 | 00000000 |
| C9 | | | 07Ch | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 11001001b=C9h. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду CMP [EDX\*4+ESI+7], ECX можно сделать вывод, что ей соответствует машинный код   
**C907000000h**. Длина команды – 5 байт.

**Машинный код 1: 8B5E 01**

(MOV rl6,r/ml6)

Первый байт: 8Bh=10001011b. Код операции 1011 соответствует команде MOV, один из операндов которой имеет регистровую адресацию, второй – по базово-индексную со смещением .Mod =1 ,смешение равно 1 байт.r/m=110,значит 4 операранд в памяти. Разложим команду на части:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **Mod** | **reg** | **r/m** | **scale** | **index** | **Base** |
| 10001011 | 1 | 011 | 110 | 01 | 000 | 000 |
| 8B h | 5Е h | | | 01h | | |

Значение поля reg=011 соответствует регистру BX. w=1, значит размер пересылаемых данных – 4 байта. Таким образом, искомая команда пересылает значение **8B5E 01**= 9133569 в регистр BX и имеет вид: MOV BX, **01**

**Машинный код 2:** 8AC3

Первый байт: 8Ah=10001010 b. Код операции 1000 соответствует команде MOV, один из операндов которой имеет регистровую адресацию, второй – непосредственную. Разложим команду на части:

|  |  |  |  |
| --- | --- | --- | --- |
| **КОП** | **w** | **reg** | **195** |
| 10001010 | 1 | 111 | 11000011 |
| 8Ah | | | C3h |

Значение поля reg=111 соответствует регистру DI. w=1, соответствует размеру двойного слова пересылаемых данных. Таким образом, искомая команда пересылает значение 195 в регистр DI и имеет вид: MOV DI, 195.

**Вывод**: В ходе лабораторной работы мы изучили структуру команд процессора и научились составлять машинный код простейших команд. Изучили такие поля как КОП, d, w, mod, reg/КОП, r/m, scale, index, base.Преобразовывали коды в машинный код и обратно.