**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 Структура команд процессора

Выполнил: ст. группы ВТ-31  
Новожен Н.В

Проверил: Осипов.О.В

**Белгород 2019**

**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).

**Вариантn 11**

**Символьное описание команд на языке Assembler**:

11. MOV ESI, 'c'

CMP BP, DI

ADD AL, [EBP+ESI+3]

SUB BYTE PTR [EBP], 45h

AND [ESI\*2], CX

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

8B441F 0E

B05A

**Команда 1: MOV ESI, 'c';63h**

Команда выполняет пересылку ASCI символа ‘**с**’ в регистр **ESI**. Первый операнд имеет регистровую адресацию, второй является непосредственным операндом. Код операции данной команды **MOV** **КОП**=1011. Размер пересылаемых данных равен 4 байта, значит **w**=1. Регистру EBX соответствует поле **reg**=110. Число кодируется следующими четырьмя байтами. 99 = 63h = 01100011b. Байты числа представляются в памяти в обратном порядке, поэтому в коде команды первым будет младший байт 01100011b=63h . Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | **828** | | | |
| 1011 | 1 | 110 | 01100011 | 00000000 | 00000000 | 00000000 |
| BE | | | 63h | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 10111110=BEh. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду MOV ESI,'c' можно сделать вывод, что ей соответствует машинный код   
**BE63000000** Длина команды – 5 байт.

**Команда 2: CMP BP, DI**

Команда выполняет Сравнение слов из регистра **BP** и **DI** и воздействует на такие флаги процессора как AF, CF, OF, PF, SF и ZF. Первый и второй операнд имеет регистровую адресацию.Для данной команды **CMP** КОП=001110. d=1, т.к. данные пересылаются из поля r/m в поле reg. Поле w=1 – пересылка слова. d=1. Регистр BP кодируется полем полем reg=101. **DI** – полем r/m=111. Операндов в памяти нет, поэтому mod=11.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **Reg** | **r/m** |
| 001110 | 1 | 1 | 11 | 101 | 111 |
| 3B | | | EF | | |

Таким образом машинный код данной команды **3**BEF. Размер команды – 2 байта.

**Команда 3: ADD AL, [EBP+ESI+3]**

Команда выполняет сложение двойных слов из регистра AL и из памяти по адресу **DS**:[ **EBP+ESI+3**] и запись результата в регистр **AL**. Первый операнд имеет регистровую адресацию, второй – базово-индексную со смещением.

Для данной команды ADD КОП=000000. d=1, т.к. данные пересылаются из поля r/m в поле reg. Поле w= 0– 1 байт. Для кодирования смещения необходимо не менее 1 байт, поэтому mod=01. Регистру AL соответствует значение reg=000. r/m = 100, так как эффективный адрес задаётся в байте SIB, который добавляется к коду команды. Поля SIB имеют значения: scale=0 0(множитель 1), index=101 (EBP), base=110 (ESI). Смещение кодируется 1 байтом. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **scale** | **index** | **Base** | **00000011b** |
| 000000 | 1 | 0 | 01 | 000 | 100 | 00 | 101 | 110 |  |
| 02h | | | 44h | | | 2Eh | | | 03h |

Размер команды – 4 байт.

**Команда 4: SUB BYTE PTR [EBP], 45h**

Команда выполняет вычитание десятичного числа 45 из ячейки памяти, адрес которой содержится в регистре EBP. Размер непосредственного операнда указан явно   
(BYTE PTR). Данной команде SUB соответствует КОП=10000000/101. Первый операнд имеет базовую адресацию, второй является непосредственным операндом. mod=01, так как поле смещения 1. r/m=101 – эффективный адрес равен значению в регистре EBP. Данная команда кодируется следующим образом:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **mod** | **КОП** | **r/m** | **Смещение - 0** | | | **Операнд – 4516** |
| 10000000 | 01 | 101 | 101 | 00 | 000 | 000 | 01000101 |
| 80h | 6Dh | | | 00h | | | 45h | |

Таким образом, машинный код данной команды 806D0045. Размер команды – 4 байта.

**Команда 5:AND [ESI\*2], CX**

Команда выполняет побитовое AND ячейки памяти по адресу **[ESI\*2** и регистра EBP. Размер непосредственного операнда указан не явно (WORD PTR). Данной команде SUB соответствует КОП=00100001. Первый операнд имеет базовую адресацию с масштабированием, второй является непосредственным операндом. mod=00, так как поле смещения 0. r/m=100 – эффективный адрес равен значению в регистре ESI. Данная команда кодируется следующим образом:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **mod** | **reg** | **r/m** | **scale** | **index** | **Base** | **0** |
| 0010101 | 00 | 001 | 100 | 01 | 110 | 101 |  |
| 21h | 0Ch | | | 75h | | | 00000000h | |

Таким образом, машинный код данной команды 210C7500000000. Размер команды – 7 байт.

8B441F 0E

**Машинный код 1: 8B441F 0E**

(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 =01 ,смешение равно 1 байт.r/m=100,значит второй операранд в памяти. Разложим команду на части:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **Mod** | **reg** | **r/m** | **scale** | **index** | **Base** | **смешение - 14** |
| 10001011 | 01 | 000 | 100 | 00 | 011 | 111 | 00001110 |
| 8B h | 44h | | | 1Fh | | | 0Eh |

Значение поля reg=000 соответствует регистру EAX. w=1, значит размер пересылаемых данных – 4 байта. Таким образом, искомая команда пересылает значение 441F0Eh= 4464398 в регистр EAX и имеет вид: MOV EAX, **[EBX+EDI+00001110]**

**Машинный код 2:** B05A

Первый байт: B0h=10110000b. Код операции 1011 соответствует команде MOV, один из операндов которой имеет регистровую адресацию, второй – непосредственную. Разложим команду на части:

|  |  |  |  |
| --- | --- | --- | --- |
| **КОП** | **w** | **reg** | **90** |
| 10110000 | 0 | 000 | 01011010 |
| B0h | | | 5Ah |

Значение поля reg=000 соответствует регистру AL. w=0, значит размер пересылаемых данных – 1 байт. Таким образом, искомая команда пересылает значение 90 в регистр AL и имеет вид: MOV AL, 90.

**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.