**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**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

тема: «Структура команд процессора»

Выполнил: ст. группы ПВ-31

Донцов А.А.

Проверил: Осипов О.В.

Белгород 2019

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

**Вариант 1**

Символьное описание команд на языке Assembler:

XOR BX, 100b

MOV DWORD PTR [EBX], 'b'

CMP [EBP+2], DL

SBB AX, DX

ADD EAX, [EBX\*8+EDI+4Ah]

8A5C2E 0C

8953 02

**Команда 1: XOR BX, 100b**

Команда выполняет операцию исключающее ИЛИ между регистром BX и числом 100b, результат записывается в BX. Первый операнд имеет регистровую адресацию, второй является непосредственным операндом. Код операции данной команды **XOR КОП**=110011. Размер пересылаемых данных равен 2 байтам, значит **w=**0. Регистру BX соответствует поле **reg**=011. Число 100b кодируется следующими двумя байтами. 4 = 4h = 100b. Байты числа представляются в памяти в обратном порядке, поэтому в коде команды первым будет младший байт 0000000010b=4h. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | **100b** | |
| 110011 | 1 | 011 | 00000100 | 00000000 |
| 33Bh | | | 4h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 1100111011b=33Bh. Непосредственный операнд кодируется следующими 2 байтами. Проанализировав команду MOV BX, 100b можно сделать вывод, что ей соответствует машинный код   
**33B400h**. Длина команды – 3 байта.

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

Команда выполняет пересылку символа b в ячейку из регистра EBX. Первый операнд имеет базовую адресацию, второй является непосредственным операндом. Код операции данной команды **MOV** **КОП**=1011. Размер пересылаемых данных равен 4 байтам, значит **w**=1. Регистру EBX соответствует поле **reg**=100. Символ b кодируется следующими четырьмя байтами. 62 = 3Eh = 111110b. Байты числа представляются в памяти в обратном порядке, поэтому в коде команды первым будет младший байт 00111110b=3Eh, следующий – 00000000b=00h. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **W** | **Reg** | **‘b’** | | | |
| 1011 | 1 | 100 | 00111110 | 00000000 | 00000000 | 00000000 |
| 3Eh | | | 3Eh | 00h | 00h | 00h |

Первые три поля **КОП, w, reg** образуют первый байт: 10111100b=BCh. Непосредственный операнд кодируется следующими 4 байтами. Проанализировав команду MOV EBX, 828 можно сделать вывод, что ей соответствует машинный код   
**3E3E000000h**. Длина команды – 5 байт.

**Команда 3: CMP [EBP+2], DL**

Команда выполняет сравнение по адресу и 8-битного регистра DL. Код операции данной команды КОП=111000. w=0, т.к. размер операндов – один байт, d=0. [EBP+2] кодируется полем r/m=001, CH – полем reg=101. Операндов в памяти нет, поэтому mod=11. Построим машинный код данной команды:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **r/m** |
| 111000 | 0 | 0 | 01 | 101 | 101 | 010 |
| 66h 38h 6Ah | | | | | | |

Таким образом машинный код данной команды 386A. Размер команды – 2 байта.

**Команда 4: SBB AX, DX**

Команда выполняет вычитание из регистра AX регистр DX. Операнды имеют регистровую адресацию. Код операции данной команды **MOV** **КОП**=11001. Размер пересылаемых данных равен 2 байтам, значит **w**=1. Регистру AX соответствует поле **reg**=000. Регистру DX соответствует поле **r/m**=010.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **reg** | **r/m** |
| 11001 | 0 | 1 | 011 | 010 |
| 66h 65h | | | | 1Ah |

**Команда 5: ADD EAX, [EBX\*8+EDI+4Ah]**

Команда выполняет сложение двойных слов из регистра EAX и из памяти по адресу [EBX\*8+EDI+4Ah] и запись результата в регистр EAX. Первый операнд имеет регистровую адресацию, второй – базово-индексную со смещением и масштабированием.

Для данной команды ADD КОП=000000. d=1, т.к. данные пересылаются из поля r/m в поле reg. Поле w=1 – пересылка двойного слова. Для кодирования смещения необходимо не менее двух байт, поэтому mod=10. Регистру EAX 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=01 (множитель 2), index=011 (EBX), base=110 (ESI). Смещение кодируется 4 байтами. Младший байт смещения 10111011b=BBh, второй – 00000010b=02h.

Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **scale** | **index** | **base** | **10 10111011b** |
| 000000 | 1 | 1 | 10 | 000 | 100 | 01 | 011 | 110 |  |
| 03h | | | 84h | | | 5Eh | | | BB02h |

**Машинный код 1:** 8A5C2E 0C

Первый байт: 8Ah=10001010b. КОП=100010 соответствует команде MOV, у которой операнды располагаются в памяти или в регистрах. Разложим команду на части:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **scale** | **index** | **base** | **12** |
| 100010 | 1 | 0 | 01 | 011 | 100 | 00 | 101 | 110 | 00001100 |
| 8Ah | | | 5Ch | | | 2Eh | | | 0Сh |

mod=01, значит размер поля смещения – 1 байт. d=1, значит первый операнд закодирован в поле reg, а второй – в r/m. w=0 соответствует 1 байтовому размеру пересылаемых данных. reg=011 соответствует регистру BL, r/m=100 говорит о наличии байта SIB. **scale**=00 – масштаб отсутствует, **index**=101 – индексный регистр **CH**, **base**=110 – базовый регистр **DH.** Байт смещения 0Ch соответствует десятичному числу 12. Машинный код 8A5C2E 0C соответствует команде **MOV BL [CH + DH + 12].**

**Машинный код 2:** 8953 02

Первый байт: 8Bh=10001001b. КОП=100010 соответствует команде MOV, у которой операнды располагаются в памяти или в регистрах. Разложим команду на части:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **2** |
| 100010 | 0 | 1 | 01 | 010 | 011 | 00000010 |
| 89h | | | 53h | | | 02h |

mod=01, значит размер поля смещения – 1 байт. d=0, значит первый операнд закодирован в поле r/m, а второй – в reg. w=1 соответствует размеру двойного слова пересылаемых данных. reg=010 соответствует регистру EDX, r/m=011 – регистру EBX. Машинный код 8953 02 соответствует команде MOV [EBX + 2], EDX.