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

по дисциплине: Архитектура вычислительных систем

тема: «Структура команд процессора»

Выполнил: ст. группы ПВ-211

Чувилко Илья Романович

Проверил:

Осипов Олег Васильевич

Белгород 2022 г.

Вариант 20

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

Задание:

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).

Символьное описание команд на языке Assembler:

1. CMP ESP, 100

2. MOV BYTE PTR [EBP], 'Q'

3. ADD AX, [ESI]

4. XOR [EBX*2+ECX+2], EDX

5. SUB CX, AX

Машинные коды команд в 16 системе счисления:

1. 83E8 22

2. 8BD8

Выполнение:

- **Символьное описание команд на языке Assembler:**

Команда 1: CMP ESP, 100

В 16х представлении: 83FC 64

В двоичном: 1000 0011 1111 1100

Команда выполняет сравнение 32-битного регистра ESP и десятичного числа 100. Код операции данной команды КОП=100000/111. w=1, т.к. размер операндов – 4 байт, d=1. Регистр ESP 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		КОП			r/m			100							
1	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	1	0	0
83h								Fch								64h							

Таким образом, машинный код данной команды 83FC64. Размер команды – 3 байта

Команда 2: MOV BYTE PTR [EBP], 'Q'

Команда выполняет пересылку символа 'Q' в ячейку по адресу [EBR]. Первый операнд имеет базовую адресацию, второй – непосредственную. Данной команде SUB соответствует КОП=11000110/000. mod=00, так как поле смещения отсутствует. r/m=101 – эффективный адрес равен значению в регистре ESI. Данная команда кодируется следующим образом:

КОП								mod		КОП			r/m			'Q'							
1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	1
C6h								05h								51h							

Таким образом, машинный код данной команды C64551. Размер команды – 3 байта

Команда 3: ADD AX, [ESI]

Команда выполняет сложение двойных слов из регистра AX и из памяти по адресу DS:[ESI] и запись результата в регистр AX. Первый операнд имеет регистровую адресацию, второй – базовую.

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. Поле смещения отсутствует, поэтому mod=00. Регистру AX соответствует значение reg=000. r/m = 110, так как эффективный адрес задаётся в байте ESI, который добавляется к коду команды.

Префикс	КОП						d	w	mod		reg			r/m		
	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0
66h	03h								06h							

Таким образом, машинный код данной команды 66:0306. Размер команды – 3 байта

Команда 4: XOR [EBX*2+ECX+2], EDX

Команда выполняет исключающего или двойных слов из регистра EDX и из памяти по адресу DS:[EBX*2+ECX+2] и запись результата в регистр по адресу DS:[EBX*2+ECX+2]. Первый операнд имеет базово-индексную адресацию со смещением и масштабированием, второй – регистровую адресацию . Для данной команды XOR КОП=001100. d=0, т.к. данные пересылаются из поля reg в поле r/m. Поле w=1 – пересылка двойного слова. Для кодирования смещения необходимо не менее двух байт, поэтому mod=10. Регистру EDX соответствует значение reg=010. 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=001 (ECX). Смещение кодируется 1 байтом: 00000010b = 02h. Поля данной команды кодируются в следующей последовательности:

КОП						d	w	mod		reg			r/m			sc		ind			base			2							
0	0	1	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	1	0
31h								54h								59h								02h							

Таким образом, машинный код данной команды 31545902. Размер команды – 4 байта

Команда 5: SUB CX, AX

Команда выполняет вычитание двойных слов из регистра CX и из регистра AX и запись результата в регистр CX. Первый и второй операнд имеет регистровую адресацию.

Для данной команды SUB КОП=001010. d=1, т.к. данные пересылаются из поля r/m в поле reg. Поле w=1 – пересылка двойного слова. Операндов в памяти нет, поэтому mod=11. Регистру CX соответствует значение reg=001. r/m = 000, так как соответствует регистру AX. Поля данной команды кодируются в следующей последовательности:

Префикс	КОП						d	w	mod		reg			r/m		
	0	0	1	0	1	0	1	1	1	1	0	0	1	0	0	0
66h	2Bh								C8h							

Таким образом, машинный код данной команды 662BC8. Размер команды – 3 байта

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

Машинный код 1: 83E8 22

Первый байт: 10000011, что соответствует операции **SUB /5 ib** у которой операнды располагаются в памяти или в регистрах. Разложим команду на части:

КОП								mod		КОП			r/m			32							
1	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	0	1	0	0	0	1	0
83h								E8h								22h							

Первый операнд имеет регистровую адресацию, второй является непосредственным операндом. Данной команде **SUB** соответствует **КОП**=10000011/101. **mod**=11, значит операндов памяти нет. **r/m**=000 соответствует регистру **AL**. Следовательно, команда имеет вид: SUB AL 32

Машинный код 2: 8BD8

Первый байт: 10001011, что соответствует операции MOV /r, это означает, что байт mod r/m команды содержит как регистровый операнд, так и операнд r/m. Разложим

команду на части:

КОП						d	w	mod		reg			r/m		
1	0	0	0	1	0	1	1	1	1	0	1	1	0	0	0
8Bh								D8h							

mod = 11, следовательно операндов памяти нет. w=1, значит размер данных 16 или 32 бита. D=1, значит первый операнд определяется полем reg, а второй r/m. Взаимодействие происходит с регистрами процессора. Reg=011, что соответствует регистру EBX. r/m=000, что соответствует регистру EAX. Следовательно, команда имеет вид: MOV EBX EAX.