**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ **«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ 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 ВТ-31

Подкопаев Антон Валерьевич

Проверил: Осипов Олег Васильевич

**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).

**Вариант 13**

MOV AX, 120h

CMP DI, AX

SUB [EBP\*8], AX

ADC CX, [ESI+101000101b]

OR BYTE PTR [EBP+EDI+8], 9

8BC8

BB 1200

**Ход выполнения работы**

.386

.MODEL FLAT, STDCALL

OPTION CASEMAP: NONE

include c:\masm32\include\windows.inc

include c:\masm32\include\kernel32.inc

include c:\masm32\include\user32.inc

includelib c:\masm32\lib\user32.lib

includelib c:\masm32\lib\kernel32.lib

.DATA

.CODE

START:

MOV AX, 120h

CMP DI, AX

SUB [EBP\*8], AX

ADC CX, [ESI+101000101b]

OR BYTE PTR [EBP+EDI+8], 9

PUSH NULL

CALL ExitProcess

END START

**Команда 1: MOV AX, 120h**

Команда выполняет пересылку шестнадцатеричного числа 120 в регистр **AX**. Первый операнд имеет регистровую адресацию, второй является непосредственным операндом.

Код операции данной команды **MOV** **КОП**=1011. Размер пересылаемых данных равен 2 байтам, значит **w**=1. К началу команды приписывется префикс 66: Регистру **AX** соответствует поле **reg**=000. Число 120 кодируется следующими двумя байтами:

120h = 100100000b. Байты числа представляются в памяти в обратном порядке, поэтому в коде команды первым будет младший байт 00100000b=20h, следующий – 00000001b=1h. Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Префикс** | **КОП** | **w** | **reg** | **120h** | |
|  | 1011 | 1 | 000 | 00100000 | 00000001 |
| 66h | B8h | | | 20h | 01h |

Первые три поля **КОП, w, reg** образуют первый байт: 10111011b=BBh. Непосредственный операнд кодируется следующими двумя байтами. Проанализировав команду **MOV AX, 120h** можно сделать вывод, что ей соответствует машинный код **66:B8 2001**. Длина команды – 4 байта.

**Команда 2:** CMP DI, AX

Команда выполняет сравнение 16-битных регистров CL и CH. Код операции данной команды КОП=001110, w=1, т.к. размер операндов – два байта. К команде приписывается префикс 66:. Байт d=1, т. к. оба операнда являются регистрами, первый определяется полем reg, второй полем r/m. Регистр DI кодируется полем reg=111, AX – полем r/m=000. Операндов в памяти нет, поэтому **mod**=11. Построим машинный код данной команды:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Префикс** | **КОП** | **d** | **w** | **mod** | **reg** | **r/m** |
|  | 001110 | 1 | 1 | 11 | 111 | 000 |
| 66h | 3Bh | | | F8h | | |

Таким образом машинный код данной команды 66:3BF8. Размер команды – 3 байта.

**Команда 3:** SUB [EBP\*8], AX

Команда выполняет вычитание слова, находящего в регистре AX, из ячейки памяти, адрес которой содержится в регистре EBP и записывает результат в EBP. Первый операнд имеет базовую адресацию с масштабированием, а второй регистровую адресацию, причем первый операнд имеет неявное приведение (WORD PTR), чтобы соответствовать размеру второго операнда.

Данной команде SUB соответствует КОП=1010, d=0, т. к. происходит пересылка данных из r/m=100, соответствующего байту SIB, в reg=000, соответствующего регистру AX. w=1, т. к. размер операндов равен 16 битам или одному слову. К команде добавляется префикс 66: mod=00, так как смещение отсутствует. **scale**=11 из-за масштабирования 8, а **index**=**base**=101, соответствуя EBP. Данная команда кодируется следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Префикс** | **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | **scale** | **index** | **base** | **0** |
|  | 001010 | 0 | 1 | 00 | 000 | 100 | 11 | 101 | 101 |  |
| 66h | 29h | | | 04h | | | EDh | | | 00000000 |

Таким образом, машинный код данной команды 66:2904ED 00000000 – 8 байт.

**Команда 4:** ADС CX, [ESI+10100010b]

Команда выполняет сложение cлов из регистра CX и из памяти по адресу DS:[ESI+ESI+10100010b] и запись результата в регистр CX. Первый операнд имеет регистровую адресацию, второй – базово-индексную со смещением. Второй операнд неявно приведен к слову (WORD PTR).

Для данной команды ADD КОП=000100. d=1, т.к. данные пересылаются из поля r/m в поле reg. Поле w=1 – пересылка слова, к команде добавляется префикс 66: Для кодирования смещения используется двойное слово, поэтому mod=10. Регистру CX соответствует значение reg=001. r/m = 110, соответствуя ESI. Смещение кодируется четыремя байтами. Байты смещения так же расположены в обратном порядке. Старший байт смещения 01000101b=45h, младший 00000001b=01h.

Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **reg** | **r/m** | | **101000101b** | | | |
| 000100 | 1 | 1 | 10 | 001 | 110 | | 01000101 | 00000001 | 00000000 | 00000000 |
| 13h | | | 44h | | | 45h | | 01h | 00h | 0h |

Проанализировав команду ADС CX, [ESI+10100010b], можно сделать вывод, что ей соответствует машинный код 66:1344 45010000. Размер команды – 7 байт.

**Команда 5:** OR BYTE PTR[EBP+EDI+8], 9

Команда выполняет команду логического ИЛИ над явно приведенным к размеру байта (BYTE PTR) адресом DS:BYTE PTR[EBP+EDI+8] и десятичным числом 9. Результат записывается по указанному адресу. Первый операнд имеет базово-индексную адресацию со смещением, а второй имеет непосредственную адресацию.

Для данной команды OR КОП=100000/001. d=0, т.к. первый операнд указывает на ячеку памяти. Поле w=0 – пересылка байта. Для кодирования смещения достаточно одного байта, поэтому mod=01. Значение r/m = 100, так как эффективный адрес задается в байте SIB. Поля SIB имеют значения: scale=00 - отсутствие множителя, index=101 (EBP), base=111 (EDI). Смещение кодируется двумя битами, так же как и непосредственный операнд.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **КОП** | **r/m** | **scale** | **index** | **base** | **8** | **9** |
| 100000 | 0 | 0 | 01 | 001 | 100 | 00 | 101 | 111 |  |  |
| 80h | | | 04h | | | 2Fh | | | 08h | 09h |

Проанализировав команду OR BYTE PTR[EBP+EDI+8], 9, можно сделать вывод, что ей соответствует машинный код 80042F 08 09. Размер команды – 5 байт.

**Машинный код 1:** 8BC8

Первый байт: 8Bh=10001011b. 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** |
| 100010 | 1 | 1 | 11 | 001 | 000 |
| 8Bh | | | F0h | | |

mod=11, значит оба операнда имеют регистровую адресацию. d=1, значит первый операнд закодирован в поле reg, а второй – в r/m. w=1 соответствует размеру двойного слова пересылаемых данных. reg=001 соответствует регистру ECX, r/m=000 – регистру EAX. Таким образом, машинный код 8BC8 соответствует команде MOV ESI, EAX.

**Машинный код 2:** BB 1200

Первый байт: BBh=10111011b. Код операции 1011 соответствует команде MOV, один из операндов которой имеет регистровую адресацию, второй – непосредственную. Разложим команду на части:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **КОП** | **w** | **reg** | 18 | |
| 1011 | 1 | 011 | 00010010 | 00000000 |
| BBh | | | 12h | 00h |

Значение поля reg=011 соответствует регистру ECX. w=1, значит размер пересылаемых данных – 4 байта. Таким образом, искомая команда пересылает значение 12h=18 в регистр ECX и имеет вид MOV BX, 18.

**Защита лабораторной**

**OR BYTE PTR [EDI\*2+8], 9**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **КОП** | **r/m** | | **scale** | **index** | **base** | | **8** | | | | | | | | **9** | |
| 100000 | 0 | 0 | 00 | 001 | 100 | | 01 | 111 | 101 | |  | |  | |  | |  | |  | |
| 80h | | | 0Ch | | | 7Dh | | | | 08h | | 00h | | 00h | | 00h | | 09h | |

**OR BYTE PTR [EDI\*2+EBP+8], 9**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **КОП** | **r/m** | | **scale** | **index** | **base** | | **8** | **9** |
| 100000 | 0 | 0 | 01 | 001 | 100 | | 01 | 111 | 101 | |  |  |
| 80h | | | 4Ch | | | 7Dh | | | | 08h | | 09h |

**OR BYTE PTR [EDI\*2+ESI+8], 9**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **КОП** | **d** | **w** | **mod** | **КОП** | **r/m** | | **scale** | **index** | **base** | | **8** | **9** |
| 100000 | 0 | 0 | 01 | 001 | 100 | | 01 | 111 | 110 | |  |  |
| 80h | | | 4Ch | | | 7Eh | | | | 08h | | 09h |