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-223

Игнатьев Артур Олегович

Проверил:

Осипов Олег Васильевич

Белгород 2024 г.

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

**Задачи**:

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).

**Задание варианта №3**

Символьное описание команд на языке Assembler:

OR DI, 11110001b

MOV DWORD PTR [EBX], 'L'

TEST AX, [EDI+4Fh]

ADC CL, AL

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

Машинные коды в 16 системе счисления:

8B5E 01

8AC3

**Выполнение работы**

**Команда 1: OR DI, 11110001b**

Команда выполняет побитовое "ИЛИ" между регистром DI и непосредственным значением 11110001b (F1h).

* Первый операнд — регистр DI, адресуется регистровым способом.
* Второй операнд — непосредственное значение, размером 2 байта (записано как F1h 00h).
* Код операции OR: КОП=000010.
* Размер данных 2 байта, поэтому w=1.
* Регистр DI кодируется полем reg=111, а r/m=000.
* Добавляется префикс 66h, указывающий на работу с 16-битными регистрами.

Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Префикс | КОП | d | w | mod | reg | r/m | Операнд |
| 66h | 000010 | 0 | 1 | 11 | 111 | 000 | F1h 00h |

Машинный код: 66 81 F8 F1 00

Длина команды: 5 байтов.

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

Команда записывает значение ASCII 'L' (4Ch) в память по адресу, хранящемуся в регистре EBX.

* Первый операнд — [EBX], адресуемый базовым способом (mod=00, r/m=011).
* Второй операнд — непосредственное значение, которое записывается как 4Ch в младший байт и 00h в остальные.
* Код операции MOV: КОП=110001.
* Размер данных 4 байта (DWORD), поэтому w=1.

Построим машинный код:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| КОП | d | w | mod | reg | r/m | Операнд |
| 110001 | 0 | 1 | 00 | 000 | 011 | 4Ch 00h 00h 00h |

Машинный код: C7 03 4C 00 00 00

Длина команды: 6 байтов.

**Команда 3: TEST AX, [EDI+4Fh]**

Команда выполняет проверку флага на основе результата логического "И" между содержимым регистра AX и значением в памяти по адресу [EDI+4Fh].

* Первый операнд — регистр AX, кодируется как reg=000.
* Второй операнд — [EDI+4Fh], адресуемый способом со смещением (mod=01, r/m=111).
* Код операции TEST: КОП=100001.
* Размер данных 2 байта, поэтому w=1.
* Для работы с 16-битными регистрами добавляется префикс 66h.

Построим машинный код данной команды:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Префикс | КОП | w | mod | reg | r/m | Операнд |
| 66h | 100001 | 1 | 01 | 000 | 111 | 4Fh |

Машинный код: 66 A9 4F

Длина команды: 3 байта.

**Команда 4: ADC CL, AL**

Команда выполняет сложение регистра AL с регистром CL, включая флаг переноса (CF).

* Первый операнд — регистр CL, кодируется как reg=001.
* Второй операнд — регистр AL, кодируется как r/m=000.
* Код операции ADC: КОП=000100.
* Размер данных 1 байт, поэтому w=0.

Поля данной команды кодируются в следующей последовательности:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| КОП | d | w | mod | reg | r/m |
| 001010 | 1 | 0 | 11 | 001 | 000 |

Машинный код: 12 C0

Длина команды: 2 байта.

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

Команда выполняет сравнение значения в памяти по адресу [EDX\*4+ESI+7] с содержимым регистра ECX.

* Первый операнд — [EDX\*4+ESI+7], адресуемый базово-индексным способом:
  + mod=01, r/m=100 (SIB).
  + В SIB: scale=10 (умножение на 4), index=010 (EDX), base=110 (ESI).
  + Смещение: 7 (1 байт).
* Второй операнд — регистр ECX, кодируется как reg=001.
* Код операции CMP: КОП=001110.
* Размер данных 4 байта, поэтому w=1.

Данная команда кодируется следующим образом:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| КОП | w | mod | reg | r/m | scale | index | base | Смещение |
| 001110 | 1 | 01 | 001 | 100 | 10 | 010 | 110 | 07h |

Машинный код: 39 44 96 07

Длина команды: 4 байта.

**Машинный код 1: 8B5E 01**

**Разбор машинного кода:**

1. **Первый байт: 8B**
   * КОП=100010 — команда MOV, работающая с регистрами или памятью.
   * d=1 — данные пересылаются из памяти (или регистра в случае регистровой адресации) в регистр.
   * w=1 — пересылаются 2 или 4 байта данных.
2. **Второй байт: 5E**
   * mod=01 — адресация со смещением, 1 байт.
   * reg=011 — это регистр EBX.
   * r/m=110 — это адрес в памяти с базовым регистром ESI.
3. **Третий байт: 01**
   * Смещение для адресации составляет 1 байт.

Разложим команду на части:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| КОП | d | w | mod | reg | r/m | Операнд |
| 100010 | 1 | 1 | 01 | 011 | 110 | 01h |

* mod=01 указывает на то, что используется адресация со смещением.
* r/m=110 обозначает, что память адресуется через регистр ESI.
* Смещение 01 добавляется к значению в регистре ESI.
* reg=011 указывает, что данные записываются в регистр EBX.

Таким образом, команда перемещает значение из адреса [ESI+1] в регистр EBX.

**Интерпретация:** MOV EBX, [ESI+1]  
**Длина команды:** 3 байта.

**Машинный код 2: 8AC3**

**Разбор машинного кода:**

1. **Первый байт: 8A**
   * КОП=100010 — команда MOV, работающая с регистрами или памятью.
   * d=1 — данные пересылаются из регистра (или памяти в случае модифицированного адреса) в регистр.
   * w=0 — пересылается 1 байт данных.
2. **Второй байт: C3**
   * mod=11 — регистровая адресация (оба операнда — регистры).
   * reg=000 — это регистр AL.
   * r/m=011 — это регистр BL.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| КОП | d | w | mod | reg | r/m |
| 100010 | 1 | 0 | 11 | 000 | 011 |

**Объяснение:**

* mod=11 указывает, что оба операнда находятся в регистрах.
* d=1 говорит, что данные передаются из регистра BL в регистр AL.
* w=0 определяет размер данных как 1 байт.

Таким образом, команда перемещает содержимое регистра BL в регистр AL.

**Интерпретация:** MOV AL, BL  
**Длина команды:** 2 байта.

**Вывод:** в ходе работы изучили структуру команд процессора, научились составлять машинный код простейших команд.