Машинно-зависимые языки программирования

Лабораторная работа №2

“Создание простейшей программы на ассемблере. Отладчик”

Теоретическая и справочная информация

Язык ассемблера — машинно-ориентированный язык программирования низкого уровня. Его команды прямо соответствуют отдельным командам процессора.

Исполняемый файл — файл, содержащий программу в виде, в котором она может быть исполнена компьютером. Перед исполнением программа загружается в память, и выполняются некоторые подготовительные операции (настройка окружения, загрузка библиотек). Основной формат исполняемых файлов в Windows - .EXE.

Компилятор – это специальная программа, которая переводит текст программы, написанный на языке программирования, в набор машинных кодов.

Компоновщик (линковщик, линкер) — инструментальная программа, которая производит компоновку («линковку»): принимает на вход один или несколько объектных модулей и собирает по ним исполняемый модуль.

Отладчик — компьютерная программа для автоматизации процесса отладки: поиска ошибок в других программах. В зависимости от встроенных возможностей, отладчик позволяет выполнять трассировку, отслеживать, устанавливать или изменять значения переменных в процессе выполнения кода, устанавливать и удалять контрольные точки или условия остановки и так далее.

Macro Assembler (MASM) — ассемблер для процессоров семейства x86. Включает компилятор, линковщик и дополнительные инструменты, в т.ч. отладчик. Другие распространённые (сейчас или в прошлом) ассемблеры - TASM, NASM, FASM и др.

.COM (англ. command) — расширение файла, в системах DOS COM-файл — простой тип исполняемого файла, при выполнении которого *данные*, *код* и стек находятся в одном и том же 16-битном сегменте. Поэтому размер файла не может превышать 65280 байт (что на 256 байт меньше размера сегмента — 2^{16} байт). COM-файлы для DOS можно выполнять в некоторых версиях Windows, а также на эмуляторах.

.COM — один из простейших форматов исполняемых файлов для процессоров семейства x86. Программа, загруженная в память для исполнения, является точной копией файла на диске.

Регистры процессора — блок ячеек памяти, образующий сверхбыструю оперативную память внутри процессора. Большинство команд процессора манипулируют данными, хранящимися в регистрах.

Система команд (также набор команд) — соглашение о предоставляемых архитектурой средствах программирования, в том числе, типах данных, наборе инструкций, системе регистров и т.д.

Система команд x86 процессора включает в себя следующие четыре основные группы команд:

- команды пересылки данных;
- арифметические команды;
- логические команды;
- команды переходов.

Регистр указателя команд (**IP, Instruction pointer**) - специальный регистр, который всегда хранит в себе смещение команды, которая будет выполнена следующей. Меняется автоматически по ходу выполнения программы и не может быть изменён программно.

Регистры общего назначения процессора (РОН) 8086. Регистры общего назначения - группа регистров, доступная для чтения/записи основными командами. Предназначены для временного хранения данных, записи параметров машинных команд, арифметической обработки и т.д. Существует всего 4 РОН: AX, BX, CX, DX. Каждый содержит в себе 16 бит и делится на 2 части по 8 бит - старшую (high, H) и младшую (low, L). Обращаться можно как к регистру целиком, так и к его половинам по отдельности.

<table>
<tr><td colspan="2">AX</td><td rowspan="2">аккумулятор - умножение, деление, обмен с устройствами ввода/вывода (команды ввода и вывода);</td></tr>
<tr><td>AH</td><td>AL</td></tr>
<tr><td colspan="2">BX</td><td rowspan="2">базовый регистр в вычислениях адреса, часто указывает на начальный адрес (называемый базой) структуры в памяти;</td></tr>
<tr><td>BH</td><td>BL</td></tr>
<tr><td colspan="2">CX</td><td rowspan="2">счетчик циклов, определяет количество повторов некоторой оперции;</td></tr>
<tr><td>CH</td><td>CL</td></tr>
<tr><td colspan="2">DX</td><td rowspan="2">определение адреса ввода/вывода, так же может содержать данные, передаваемые для обработки в подпрограммы.</td></tr>
<tr><td>DH</td><td>DL</td></tr>
</table>

Основные команды

MOV - команда пересылки. Формат: MOV <приёмник>, <источник>. Записывает значение, хранящееся в источнике, в приёмник. Источником может быть константа, регистр или адрес в памяти. Приёмником - регистр или адрес в памяти.
ADD, SUB, MUL, DIV - команды сложения, вычитания, умножения, деления.

Практическое задание

1. Создайте файл hello.asm с текстом

```
.MODEL TINY
.DOSSEG
.DATA
        MSG   DB  "Hello, World!", 0Dh, 0Ah, '$'
.CODE
.STARTUP
        MOV   AH, 09h
        MOV   DX, OFFSET MSG
        INT     21h
        MOV   AH, 4Ch
        INT     21h
END
```

2. Запустите ML.EXE /AT hello.asm.
3. Посмотрите, какие файлы были созданы компилятором. Определите их размер. Просмотрите файл в любом hex-viewer’е, проанализируйте содержимое файла и изучите возможности просмотровщика.
4. Запустите скомпилированную программу.
5. Запустите AFDPRO.EXE HELLO.COM.
6. Изучите возможности отладчика: шаг с заходом, шаг с обходом, перезапуск программы, создание точек останова, наблюдение за регистрами. Справочная информация по отладчику есть в файле ASM1_AFD.pdf (выполнять задание из него не нужно).