\_00\_汇编程序运行环境介绍

**1.DOSBox**

(1)DOSBox介绍

DOSBox是一个模拟器，用于模拟80x86系列计算机的DOS系统。

它可以在现代的操作系统（如Windows、Linux、macOS等）上模拟旧的DOS环境，从而允许用户在这些系统上运行旧的DOS程序。

它不仅提供旧的DOS环境，而且可以模拟出一个完整的 IBM PC 兼容机，包括 CPU、内存、硬盘、显卡、声卡等硬件设备的运行。

(2)DOSBox进入汇编环境

指令：

**mount c d:\masm // 将masm文件夹挂载到虚拟c盘**

**c: // 进入c盘**

**debug // 执行masm提供的debug等指令**

注意：

挂载指令格式：**mount 盘服名 masm的文件路径**

以上指令的盘服是DOSBox中创建的虚拟盘服，该盘服名为a-z都可以。

**2.MASM**

(1)MASM介绍

MASM（Microsoft Macro Assembler）是微软公司研发的汇编语言开发工具。

它支持80x86汇编，可以对汇编代码进行汇编、链接、调试等操作。

(2)MASM中常用的.exe文件

①masm.exe：用于将.asm结尾的汇编语言源文件汇编为.obj结尾的二进制文件。

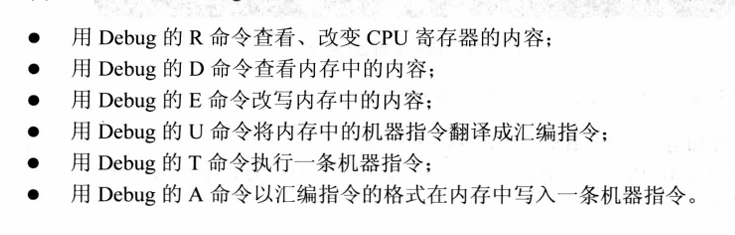
②link.exe：用于将一个或多个.obj目标文件进行链接，生成.exe结尾的可执行文件。

③debug.exe：用于调试.exe可执行文件，也可以用其直接编写汇编代码。

(补充：.asm汇编文件，先汇编为.obj文件，后链接为.exe文件，之后即可执行)

(3)debug的使用

Debug中的常用指令如下：



指令讲解：

①R指令（register）：寄存器指令

语法：R; 可查看cpu寄存器中的内容。

语法：R 寄存器名; 可向修改指定寄存器中的值。

②D指令（dump）：内存指令

语法：D; 可查看内存中的值。

语法：D 段地址:偏移地址; 可查看指定地址的内存中的值。

③A指令（assemble）：写入汇编代码指令

语法：A; 向默认CS:IP写入汇编代码。

语法：A 段地址:偏移地址; 向指定CS:IP写入汇编代码。

④T指令（trace）：执行汇编代码指令

语法：T; 执行（地址为CS:IP的）汇编代码；

⑤G命令（go）：执行到断点

语法：G 段地址:偏移地址 （此处的地值是断点，该断点是之后会执行到的指令地址CS:IP）

功能：直接把程序执行到指定断点处。

⑥P命令（pass）：执行完当前这条指令（极其子程序）。

语法：P

功能：强制执行完当前这条语句（极其子程序），并跳到下一条语句。P指令常用于直接执行完整个循环语句。

注意：T和P都是执行语句，区别是T只执行1次本条语句；而P会执行完全部本条语句（例如直接执行完整个循环），再进入下一条语句。