



哈爾濱工業大學 深圳研究生院
Harbin Institute of Technology Shenzhen Graduate School

汇编语言程序设计

实验一：熟悉汇编程序开发环境

卢光明

课程QQ群： 605283663 (17-汇编HITSZ)

汇编语言程序设计—上机实验

◆ 实验课程安排

- 共8个课时，4次实验课。

周次	星期	节次	实验室
3	2	第三节-第四节	网络与信息安全实验室 (T2604-T2606)
4	5	第九节-第十节	网络与信息安全实验室 (T2604-T2606)
5	2	第三节-第四节	网络与信息安全实验室 (T2604-T2606)
7	2	第三节-第四节	网络与信息安全实验室 (T2604-T2606)

◆ 要求

- 第一次实验，使用开发环境DOSBox+MASM。
- 评分标准：每次实验总分100，四次实验总分400，期末成绩实验占50%，四次实验成绩折算后计入总成绩。
- 课堂上**必做题**验收通过的不用提交实验报告，课堂上未完成必做题验收的，必须提交实验报告。
- 选做题每做一道加20分，但实验总分上线仍为400分。

汇编语言程序设计—上机过程

◆ 第一步：建立源程序

可以用任何一款熟悉的文本编辑器建立，编辑汇编语言源程序。但是文件名的扩展名必须是.ASM。

◆ 第二步：汇编

将源程序翻译成由机器代码组成的目标模块文件的过程。目标模块文件后缀一般为.obj。

◆ 第三步：连接

连接产生的目标模块，解决外部交叉调用，产生一个可重定位的装入模块，以及产生可选的内存映像文件。连接成功生成EXE文件。

◆ 第四步：运行检验

检验运行结果是否也目标需求相符。

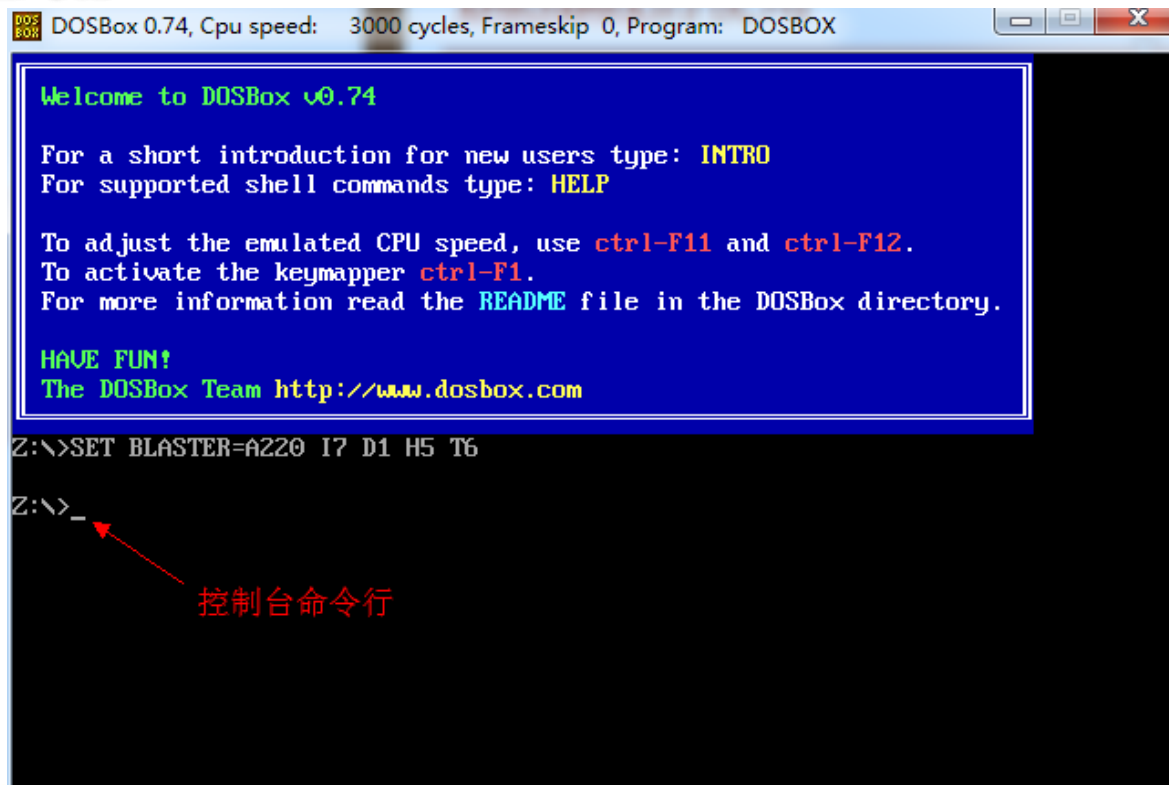
DoSBox的使用

◆ 运行DOSBox

双击桌面上的DOSBox快捷方式，运行DOSBox。

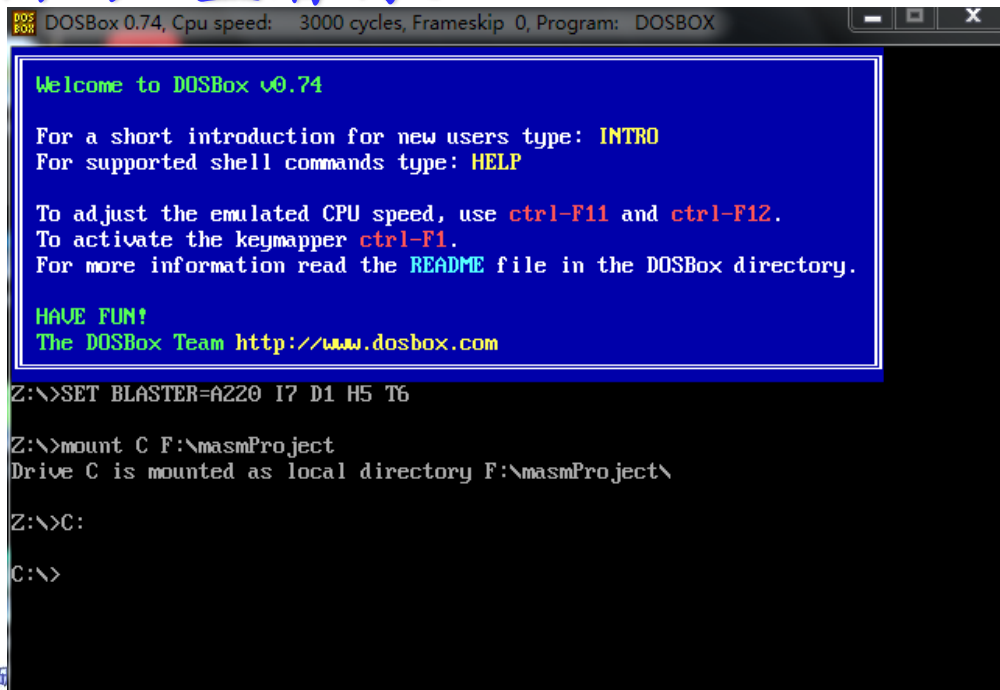


◆ 认识DOSBox



DoSBox的使用—上机过程

- ◆ 挂接：
- ◆ mount C F:\masmProject
- ◆ C:
- ◆ DoSBox就会把所建立的文件夹当做它模拟的DOS系统里面的C盘看待。



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

Welcome to DOSBox v0.74

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox directory.

HAVE FUN!
The DOSBox Team http://www.dosbox.com

Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>mount C F:\masmProject
Drive C is mounted as local directory F:\masmProject\

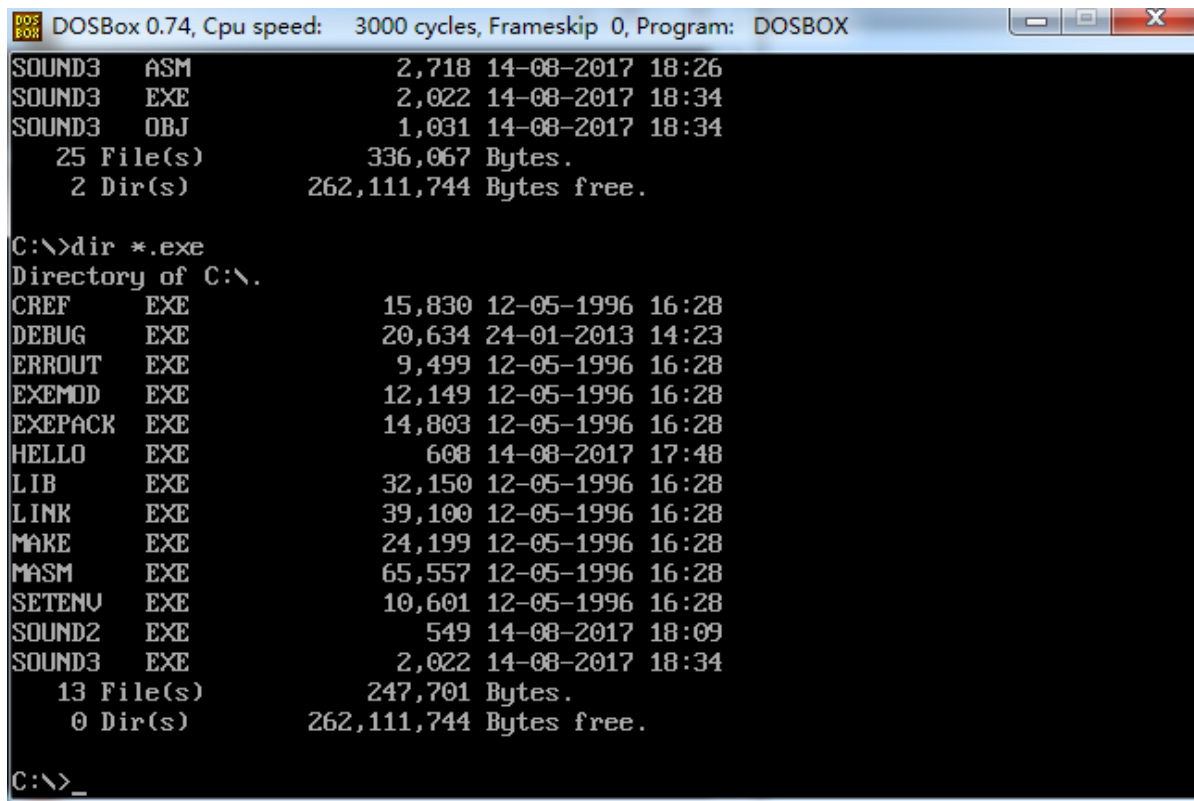
Z:\>C:

C:\>
```

汇编语言程序—上机过程

MASM5.0中四个重要的EXE文件:

1. EDIT.COM: 编辑源程序
2. MASM.EXE: 对源程序进行汇编以生成目标程序
3. LINK.EXE: 对目标程序进行连接以生成可执行程序
4. DEBUG.EXE: 对可执行程序进行调试已检验其正确性



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

SOUND3  ASM                2,718 14-08-2017 18:26
SOUND3  EXE                2,022 14-08-2017 18:34
SOUND3  OBJ                1,031 14-08-2017 18:34
    25 File(s)                336,067 Bytes.
    2 Dir(s)                262,111,744 Bytes free.

C:\>dir *.exe
Directory of C:\.
CREF    EXE                15,830 12-05-1996 16:28
DEBUG   EXE                20,634 24-01-2013 14:23
ERROUT  EXE                 9,499 12-05-1996 16:28
EXEMOD  EXE                12,149 12-05-1996 16:28
EXEPACK EXE                14,803 12-05-1996 16:28
HELLO   EXE                 608 14-08-2017 17:48
LIB     EXE                32,150 12-05-1996 16:28
LINK    EXE                39,100 12-05-1996 16:28
MAKE    EXE                24,199 12-05-1996 16:28
MASM    EXE                65,557 12-05-1996 16:28
SETENV  EXE                10,601 12-05-1996 16:28
SOUND2  EXE                 549 14-08-2017 18:09
SOUND3  EXE                2,022 14-08-2017 18:34
    13 File(s)                247,701 Bytes.
    0 Dir(s)                262,111,744 Bytes free.

C:\>_
```

汇编语言程序—上机过程

- ◆ 列表文件（扩展名为.LST）：把源程序和目标程序列表，以供检查程序用。
- ◆ 交叉索引文件（扩展名为 .CRF）：它是一个对源程序所用的各种符号进行前后对照的文件。
- ◆ 映像文件（扩展名为 .MAP）：是一种文本文件，列出各段在存储器中的分配情况。

```
DOS FOR DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

C:\>masm hello.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [hello.OBJ]:
Source listing [NUL.LST]: hello.lst
Cross-reference [NUL.CRF]: hello.crf

50632 + 465912 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link hello

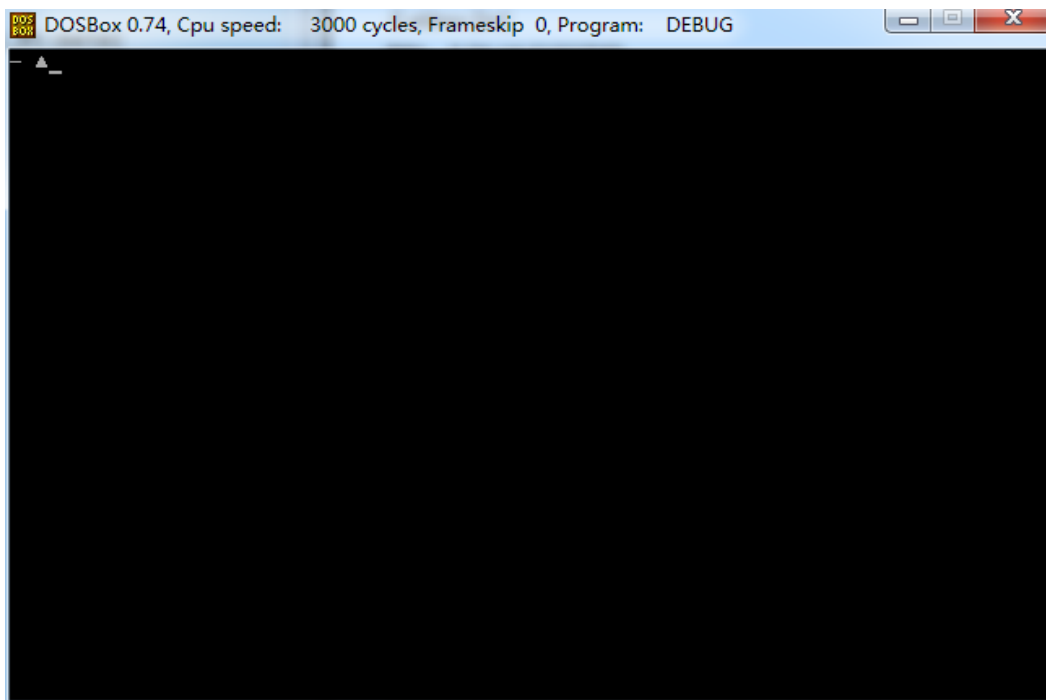
Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [HELLO.EXE]:
List File [NUL.MAP]: hello.map
Libraries [.LIB]:
LINK : warning L4021: no stack segment

C:\>dir hello
```

汇编语言程序—上机过程

调试工具：Debug



注意：debug命令在64位操作系统中不能直接运行。

解决方法：先安装DOSBox程序，然后在DOSBox环境下运行debug程序。

步骤：1) 先安装DOSBox程序；2) 将debug.exe文件保存在磁盘的根目录（如C盘）；3) 打开已经安装好的DOSBox，输入命令：mount c c:\；4) 在DOSBox环境下运行debug程序。

汇编语言程序—上机过程

Debug命令:

名称	解释	格式
a (Assemble)	逐行汇编	a [address]
c (Compare)	比较两内存块	c range address
d (Dump)	内存16进制显示	d [address]或 d [range]
e (Enter)	修改内存字节	e address [list]
f (fin)	预置一段内存	f range list
g (Go)	执行程序	g [=address][address...]
h (Hexavithmetic)	制算术运算	h value value
i (Input)	从指定端口地址输入	i pataddress
l (Load)	读盘	l [address [driver sector>
m (Move)	内存块传送	m range address
n (Name)	置文件名	n filespec [filespec...]
o (Output)	从指定端口地址输出	o portadress byte
q (Quit)	结束	q
r (Register)	显示和修改寄存器	r [register name]
s (Search)	查找字节串	s range list
t (Trace)	跟踪执行	t [=address] [value]
u (Unassemble)	反汇编	u [address]或range
w (Write)	存盘	w [address[driver sector secnum>
?	联机帮助	?

必须掌握

汇编语言程序—上机过程

上机过程总结:

**MASM5.0+DosBox:
EDIT.COM, MASM.EXE,
LINK.EXE**

调试
工具

DEBUG

**MASM for Windows 集成
实验环境(内嵌DosBox)**

**以MASM for
Windows 为主**

汇编语言程序设计—上机过程

◆ 本次实验在以上实验内容明确的前提下，实现以下必做题。

1. 编写hello.asm文件，实现输出Hello World!
2. 例程：在Y中存放着16位数，试编制一个程序把Y中1的个数存入COUNT单元中。要求改错：correct.asm程序至少有几处语法性错误，按照汇编语言语法要求进行修改并说明错误原因。并在debug模式下，修改程序运行结果。

汇编语言程序设计—上机过程

◆ 选做题1。

- 编写程序sum.asm，实现150+200的求和，结果保存在RES单元，即 $RES=X+Y$ ，其中 $X=150$ ， $Y=200$ 。数据段定义如下：

DATASG SEGMENT

X DW 150

Y DW 200

RES DW ?

DATASG ENDS

结果按照下图所示展示（但报告中要体现调试过程）：

```
-d ds:0
0770:0000  96 00 C8 00 5E 01 00 00-00 00 00 00 00 00 00 00  .....^
0770:0010  B8 70 07 8E DB A1 00 00-03 06 02 00 A3 04 00 B8  .....p
0770:0020  00 4C CD 21 00 00 00 00-00 00 00 00 00 00 00 00  .....L.
0770:0030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
0770:0040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
0770:0050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
0770:0060  00 00 00 00 00 00 00 00-00 00 0F 00 71 07 A6 01  .....q
0770:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
- _
```

汇编语言程序设计—上机过程

◆ 选做题2。

- 编写汇编程序formu.asm，实现公式 $\frac{(W-X) \times 10 + 5}{X+Y}$ ，其中数据段定义如下：

dataseg segment

DATA DB 5,10

X DB 2

Y DB 8

W DB 10

sum1 DB ? ;保存商

sum2 DB ? ;保存余数

dataseg ends ;数据段结束

结果按照如下图所示展示（但报告中要体现调试过程）：

```
-d ds:0
0770:0000  05 0A 02 08 0A 08 05 00-00 00 00 00 00 00 00 00  .....
0770:0010  B8 70 07 8E D8 A0 04 00-2A 06 02 00 F6 26 01 00  .p.....*...&..
0770:0020  02 06 00 00 8A 0E 02 00-02 0E 03 00 F6 F1 A2 05  .....
0770:0030  00 8B 26 06 00 B4 4C CD-21 00 00 00 00 00 00 00  ..&...L.!?.....
0770:0040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
0770:0050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
0770:0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
0770:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
```

汇编语言程序设计—上机过程

```
C:\>debug HELLO.EXE
-u
076F:0000 B86A07      MOV     AX,076A
076F:0003 8ED8          MOV     DS,AX
076F:0005 B409          MOV     AH,09
076F:0007 BA0000      MOV     DX,0000
076F:000A CD21          INT     21
076F:000C B44C          MOV     AH,4C
076F:000E CD21          INT     21
~
-g 0C
AX=096A BX=0000 CX=0060 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=0769 CS=076F IP=000C  NV UP EI PL NZ NA PO NC
076F:000C B44C          MOV     AH,4C
-d ds:0
076A:0000 48 65 6C 6C 6F 20 57 6F-72 6C 64 21 24 00 00 00  Hello World!$.
076A:0010 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0020 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0030 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0040 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0050 B8 6A 07 8E D8 B4 09 BA-00 00 CC 21 B4 4C CD 21  .j.....!.L.!
076A:0060 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0070 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
-e 03
076A:0003 6C.21
-d ds:0
076A:0000 48 65 6C 21 6F 20 57 6F-72 6C 64 21 24 00 00 00  Hel!o World!$.
076A:0010 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0020 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0030 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0040 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0050 B8 6A 07 8E D8 B4 09 BA-00 00 CC 21 B4 4C CD 21  .j.....!.L.!
076A:0060 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
076A:0070 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  .....
```

U反汇编指令

g执行指令

d内存16进制
显示指令

e修改内存字节
指令

谢谢！