

汇编语言程序设计

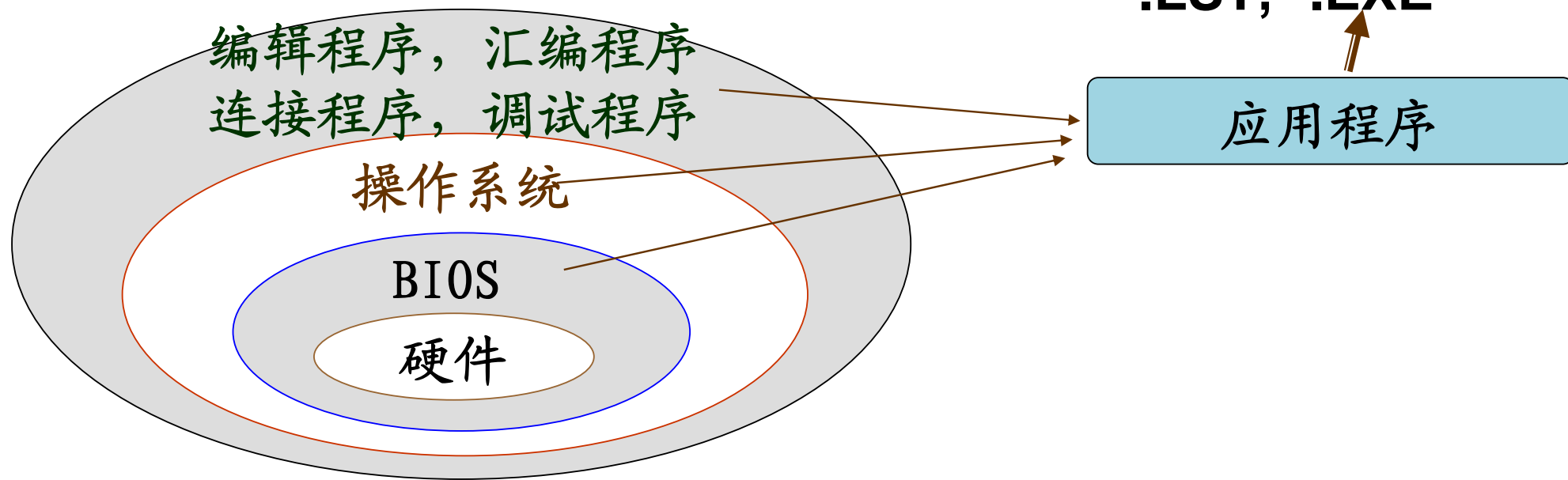
# MASM开发软件



# 软件系统

➤ Windows操作系统平台

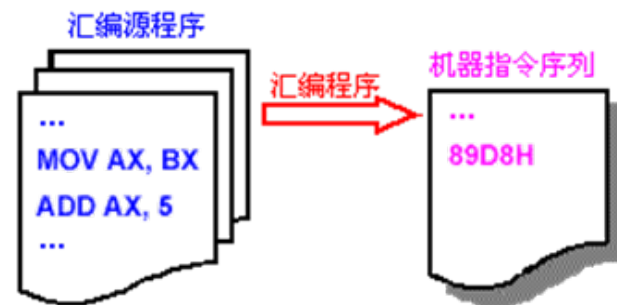
➤ MASM 6.15汇编程序



# 汇编程序（Assembler）

- 汇编程序将汇编语言源程序转换为机器代码
- 微软宏汇编程序**MASM**
  - ▶ **MASM 6.11**是最后一个独立发行的**MASM**软件包
  - ▶ **MASM 6.15**来自**Visual C++6.0**  
(支持到**Pentium 4**的**SSE2**指令系统)

汇编语言程序与汇编程序  
是两个不同的概念



# 开发软件包

- 基本开发软件环境（取自MASM 6.11和Visual C++ 6.0）
  - ▶ MASM主目录：本书I/O库、包含文件及批处理文件
  - ▶ BIN子目录：进行汇编、连接及配套程序文件
  - ▶ HELP子目录：MASM 6.11帮助文件
  - ▶ WINDBG子目录：Windows调试程序
  - ▶ PROGS子目录：示例程序或用户程序
- 建议安装到D分区的MASM目录



# BIN子目录的主要软件

## ➤ MASM 6.15 汇编程序

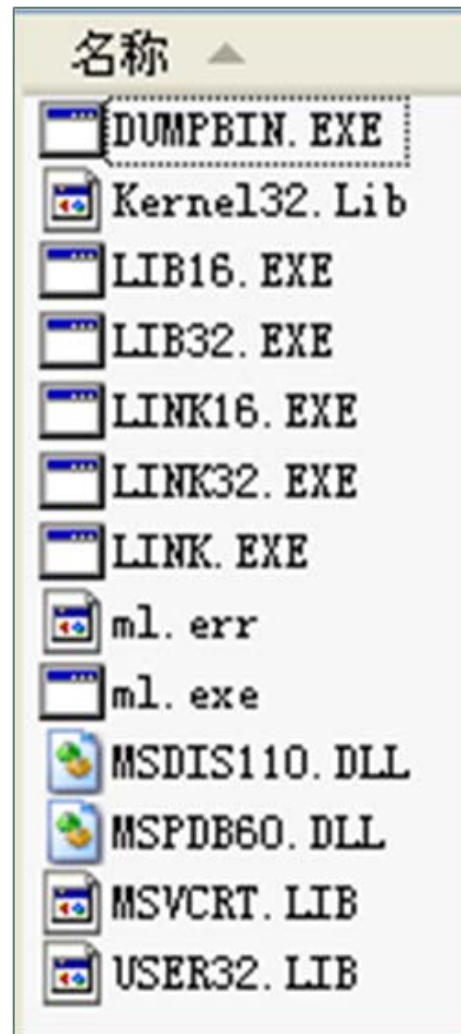
- ▶ ml.exe      主程序文件
- ▶ ml.err      错误信息文件

## ➤ 连接程序 (Linker)

- ▶ link16.exe    16位DOS连接程序
- ▶ link32.exe    32位Windows连接程序

## ➤ 子程序库管理程序

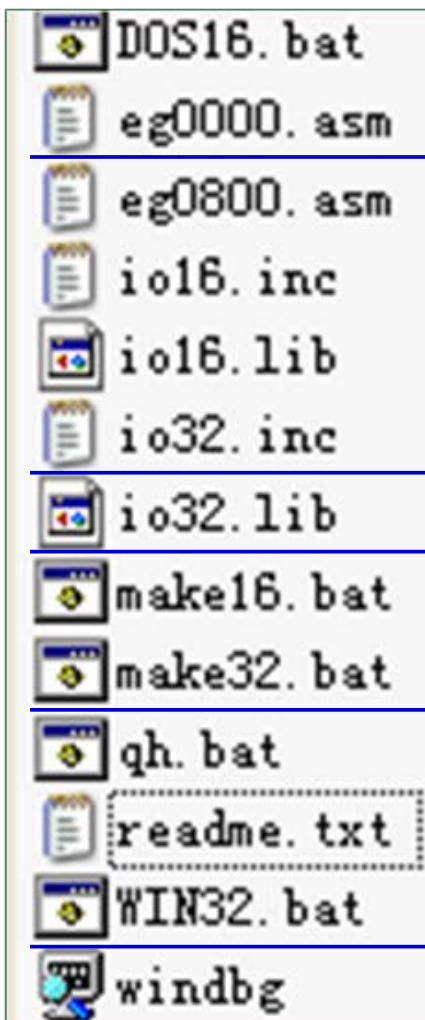
- ▶ lib16.exe    16位DOS库管理程序
- ▶ lib32.exe    32位Windows库管理程序



# MASM主目录的主要软件

## ➤ 应用于32位Windows平台的文件

- ▶ `eg0000.asm`      源程序模板文件
- ▶ `io32.inc`      32位包含文件
- ▶ `io32.lib`      32位I/O子程序库文件
- ▶ `make32.bat`      32位应用程序快速创建文件
- ▶ `WIN32.bat`      快速进入32位控制台文件
- ▶ `windbg`      调试程序的快捷方式

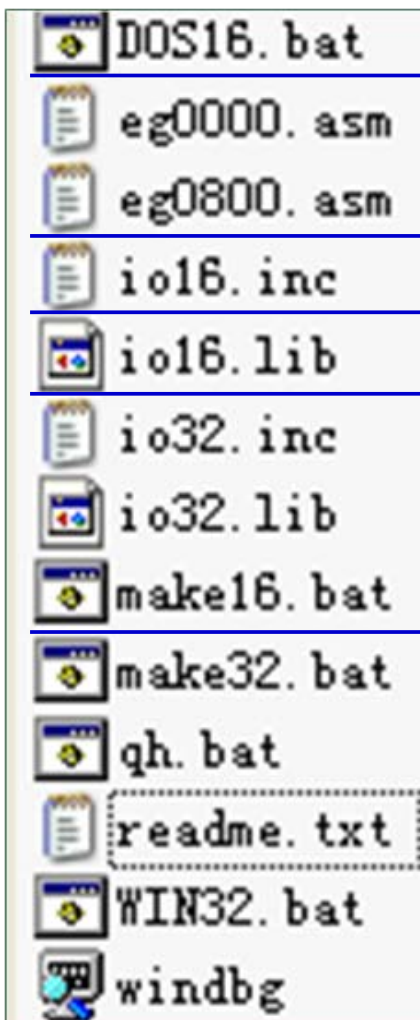




# MASM主目录的主要软件（DOS环境）

## ➤ 应用于16位DOS环境的文件

- ▶ DOS16. bat      快速进入16位DOS环境文件
- ▶ eg0800. asm      源程序模板文件
- ▶ io16. inc      16位包含文件
- ▶ io16. lib      16位I/O子程序库文件
- ▶ make16. bat      16位应用程序快速创建文件



# MASM开发软件包

本地磁盘 (D:)

MASM

bin

HELP

progs

windbg

名称

DUMPBIN.EXE

Kernel32.Lib

LIB16.EXE

LIB32.EXE

LINK16.EXE

LINK32.EXE

LINK.EXE

ml.err

ml.exe

MSDIS110.DLL

MSPDB60.DLL

MSVCRT.LIB

USER32.LIB

DOS16.bat

eg0000.asm

eg0800.asm

io16.inc

io16.lib

io32.inc

io32.lib

make16.bat

make32.bat

qh.bat

readme.txt

WIN32.bat

windbg



汇编语言程序设计

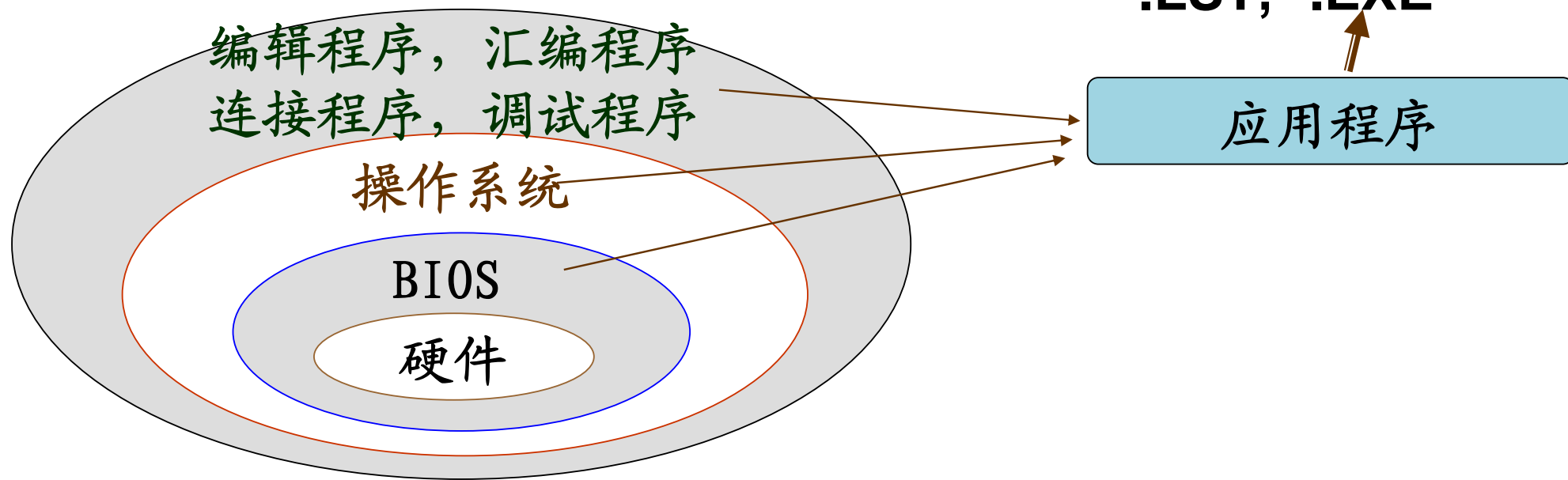
# 操作系统平台



# 软件系统

➤ Windows操作系统平台

➤ MASM 6.15汇编程序



# 操作系统（Operating System）

- 操作系统管理着系统的软硬件资源
  - ▶ 为用户提供使用机器的交互界面
  - ▶ 为程序员使用资源提供可供调用的驱动程序
  - ▶ 为其他程序构建稳定的运行平台
- 本课程基于**32位Windows**控制台环境（命令提示符）  
**%SystemRoot%\system32\cmd.exe**



# 打开命令提示符

## ➤方法1

单击“开始→程序→附件→命令提示符”

## ➤方法2

单击“开始→运行”，输入“**CMD**”

常被人称为DOS窗口？

A screenshot of the Windows XP Command Prompt window. The title bar is blue with the text "C:\ 命令提示符". The main area is black with white text. It displays "Microsoft Windows XP [版本 5.1.2600]" and "<C> 版权所有 1985-2001 Microsoft Corp.". The current directory is "C:\Documents and Settings\Administrator>".

```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
<C> 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>
```



# 32位Windows控制台和16位模拟DOS窗口



```
C:\ 命令提示符

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>
```

← 32位Windows控制台

两种环境的基本功能和界面一致，但本质不同

16位模拟DOS窗口 →



```
Command Prompt

Microsoft(R) Windows DOS
(C) Copyright Microsoft Corp 1990-2001.

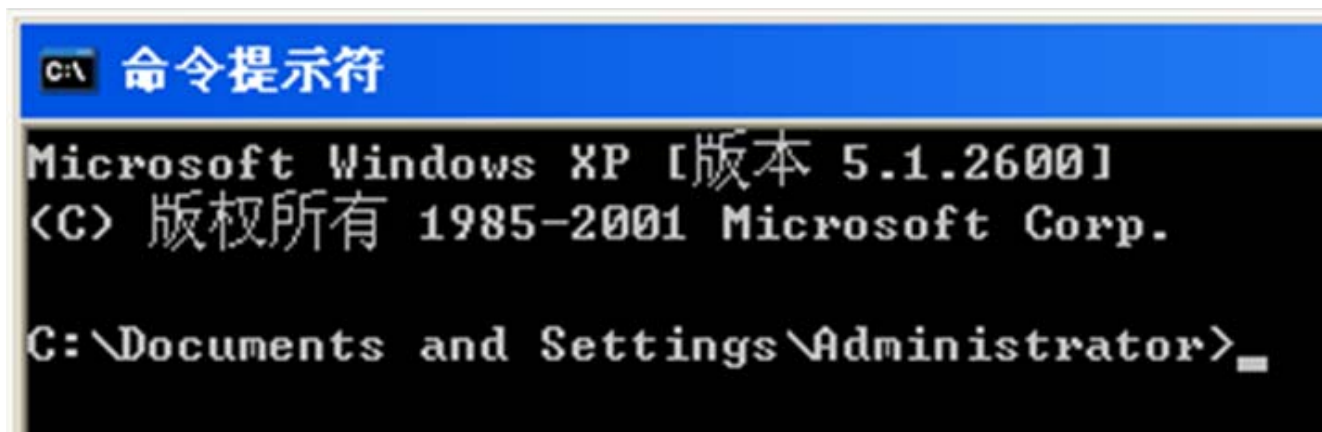
C:\DOCUME~1\ADMINI~1>
```



# 32位Windows控制台（Console）

## ➤ 32位Windows控制台（命令提示符）

**%SystemRoot%\system32\cmd.exe**

A screenshot of the Windows XP Command Prompt window. The title bar is blue with the text 'C:\ 命令提示符'. The main window has a black background with white text. It displays the Windows XP version information: 'Microsoft Windows XP [版本 5.1.2600]', the copyright notice: '<C> 版权所有 1985-2001 Microsoft Corp.', and the current directory: 'C:\Documents and Settings\Administrator>'.

```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
<C> 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>
```

基于Windows操作系统的命令行交互方式  
支持汉字等更多的功能， .....

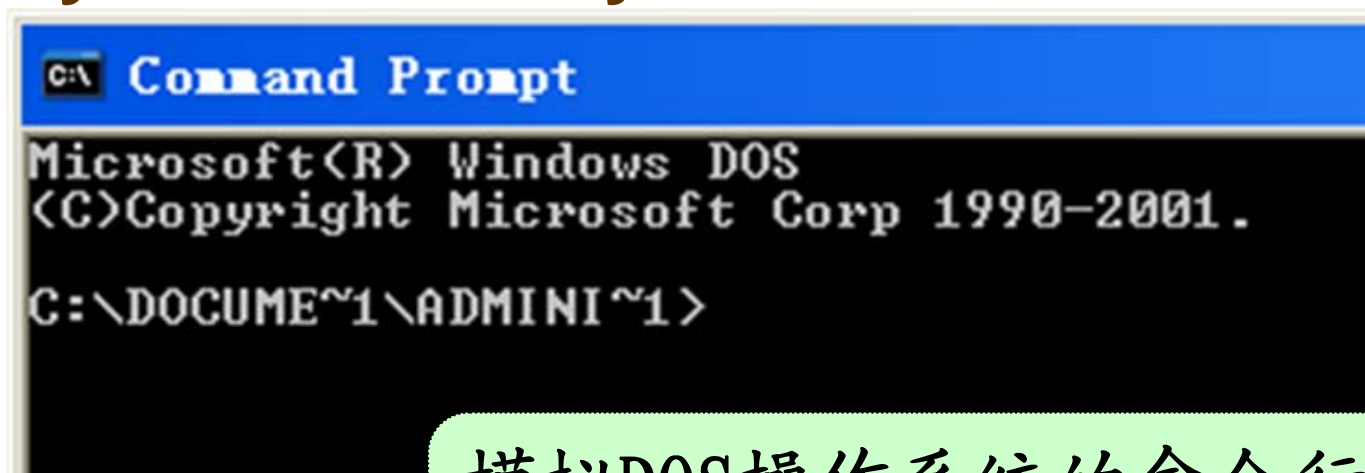




# 16位模拟DOS窗口

## ➤ 16位模拟DOS环境（Command Prompt）

**%SystemRoot%\system32\command.com**



模拟DOS操作系统的命令行交互方式  
不支持汉字、长文件名等功能， .....



# 进入MASM目录

➤ 为便于进入MASM目录，可创建批处理文件

▶ 32位Windows控制台：WIN32.BAT

▶ 16位DOS环境：DOS16.BAT

➤ 为便于访问其中文件，增加搜索路径：

```
@set PATH=D:\MASM;D:\MASM\BIN;%PATH%
```

在Windows资源管理器打开文件夹“D: \MASM”，  
双击该批处理文件，就可以进入MASM环境



# 具有搜索路径的批处理文件

## WIN32.BAT

```
@echo off
```

```
@set PATH=D:\MASM;D:\MASM\BIN;%PATH%  
%SystemRoot%\system32\cmd.exe
```

```
@echo on
```

## DOS16.BAT

```
@echo off
```

```
@set PATH=D:\MASM;D:\MASM\BIN;%PATH%  
%SystemRoot%\system32\command.com
```

```
@echo on
```



# 本讲总结

- 相对操作简单的触屏、图形界面来说
  - ▶ 字符输入的命令行虽然单调，却是最基本的交互方式
  - ▶ 可以更深刻理解目录结构、文件路径等本质内容

A screenshot of a Windows XP Command Prompt window. The title bar is blue and contains the text 'C:\WINDOWS\system32\cmd.exe'. The main window has a black background with white text. It displays 'Microsoft Windows XP [版本 5.1.2600]' and '<C> 版权所有 1985-2001 Microsoft Corp.' followed by a blank line and the prompt 'D:\MASM>'.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
<C> 版权所有 1985-2001 Microsoft Corp.

D:\MASM>
```

A screenshot of a Windows DOS Command Prompt window. The title bar is blue and contains the text 'C:\ Command Prompt'. The main window has a black background with white text. It displays 'Microsoft(R) Windows DOS' and '<C>Copyright Microsoft Corp 1990-2001.' followed by a blank line and the prompt 'D:\MASM>'.

```
C:\ Command Prompt
Microsoft(R) Windows DOS
<C>Copyright Microsoft Corp 1990-2001.

D:\MASM>
```



汇编语言程序设计

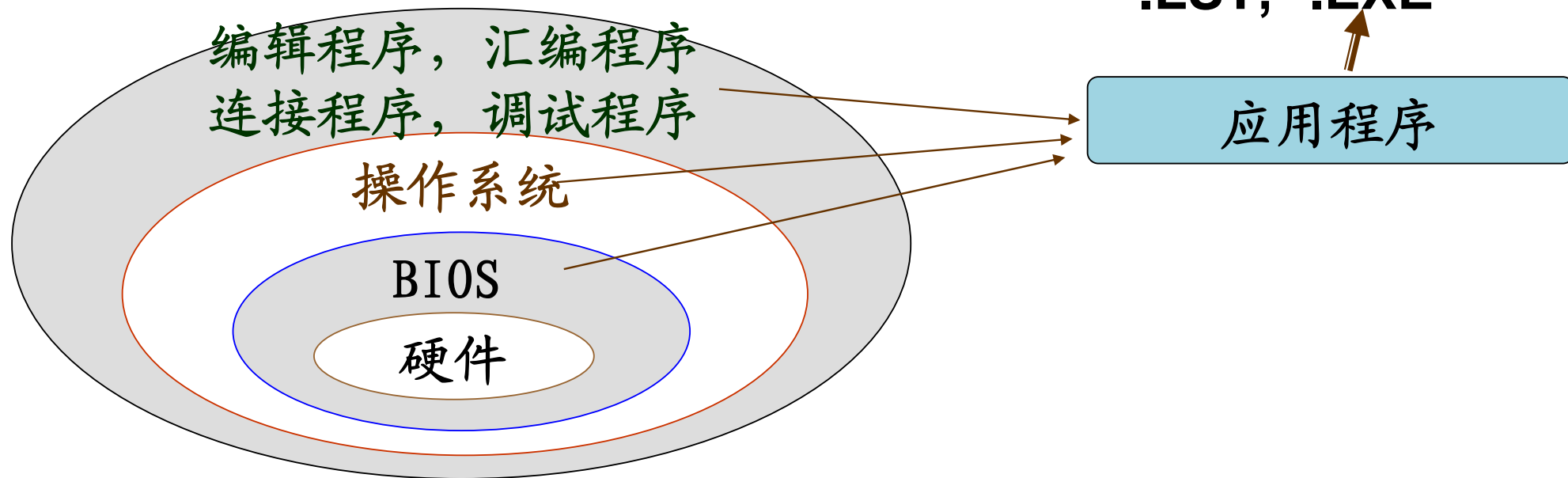
# 源程序开发过程



# 软件系统

➤ Windows操作系统平台

➤ MASM 6.15汇编程序





# MASM开发软件包

本地磁盘 (D:)

MASM

bin

HELP

progs

windbg

名称

DUMPBIN.EXE

Kernel32.Lib

LIB16.EXE

LIB32.EXE

LINK16.EXE

LINK32.EXE

LINK.EXE

ml.err

ml.exe

MSDIS110.DLL

MSPDB60.DLL

MSVCRT.LIB

USER32.LIB

DOS16.bat

eg0000.asm

eg0800.asm

io16.inc

io16.lib

io32.inc

io32.lib

make16.bat

make32.bat

qh.bat

readme.txt

WIN32.bat

windbg

# 汇编语言源程序文件eg0101.asm

**;eg0101.asm**

**include io32.inc**

**.data** ;数据段

**msg byte 'Hello, Assembly!',13,10,0**

**.code** ;代码段

**start:** ;程序执行起始位置

**mov eax,offset msg**

**call dispmsg**

**exit 0** ;程序正常执行终止

**end start** ;汇编结束

运行结果

Hello, Assembly !



# 快速开发方法

## ➤ 进入MASM开发目录

- ▶ 在Windows资源管理器打开文件夹 “D:\MASM”
- ▶ 双击批处理文件 “WIN32.BAT”

## ➤ 汇编连接、生成可执行文件

- ▶ 在命令行下输入 “MAKE32 eg0101”

## ➤ 启动可执行文件、验证程序运行正常

- ▶ 在命令行下输入 “eg0101.exe”



# 快速开发步骤

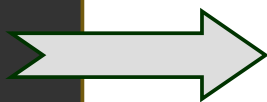
双击启动

**WIN32.BAT**



进入MASM目录

D:\MASM>



输入创建命令，生成可执行文件

D:\MASM>make32 eg0101



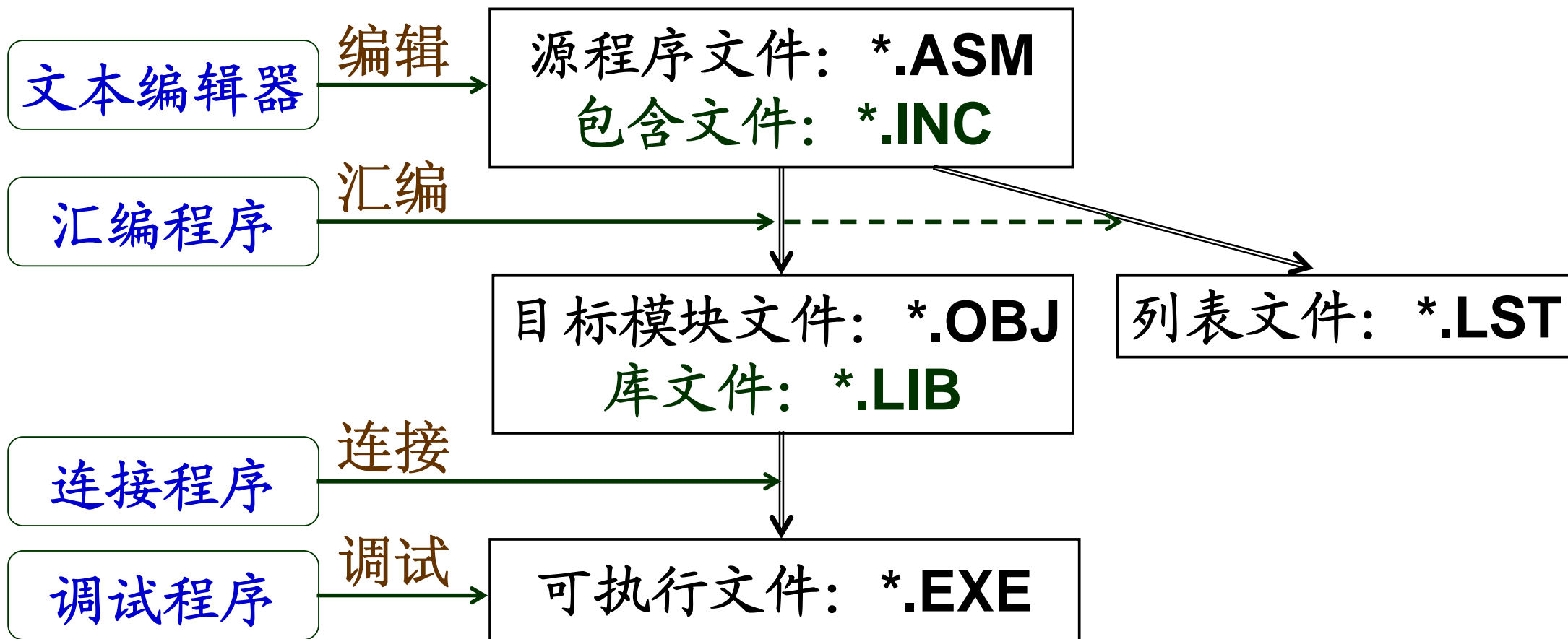
输入可执行文件名，显示运行结果

D:\MASM>eg0101.exe

Hello, Assembly !



# 开发过程



# 源程序的编辑

- 源程序文件是无格式文件、纯文本类型
- 以 **.ASM** 为扩展名，可使用任何文本编辑器
  - ▶ Windows 的记事本 Notepad
  - ▶ 其他程序开发工具中的编辑环境
  - ▶ 专注于源程序编写的编辑软件，例如 UltraEdit32
- 开发软件 MASM 主目录提供
  - ▶ Notepad2.exe 程序





# 源程序的汇编

- 生成目标模块文件（.OBJ）
- MASM 6.x的汇编程序是ML.EXE

BIN\ML /c /coff eg0101.asm

- ▶ 参数“/c”（小写字母）实现源程序的汇编
- ▶ 参数“/coff”（小写字母）生成COFF格式目标模块文件

温馨提示： **ML.EXE**的参数区别大小写

温馨提示： 将源文件放在**MASM**目录



# 目标文件的连接

- 把一个或多个目标文件和库文件合成一个可执行文件
- 可执行文件以 **.EXE** 为扩展名
- 32位连接程序被更名为 LINK32.EXE

`BIN\LINK32 /subsystem:console eg0101.obj`

- ▶ “/subsystem:console” 生成Windows控制台（Console）文件
- ▶ “/subsystem:windows” 生成Windows图形窗口的可执行文件

**温馨提示：** 使用批处理文件方便操作

**温馨提示：** 汇编程序只指出语法错误



# 可执行文件的运行

- 进入控制台（或模拟DOS）环境
- 在命令行提示符下输入文件名（可以省略扩展名）  
按下回车键运行

eg0101.exe

- 运行错误，就需要
  - ▶ 静态排错：阅读分析源程序
  - ▶ 动态排错：利用调试程序

**温馨提示：**不要在Windows下双击运行



# 列表文件

- 列表文件（.LST）含有源程序和目标代码

BIN\ML /c /coff /F1 eg0101.asm

- ▶ “/F1” 创建列表文件（大写F、小写1，不是数字1）

- 列表文件有两部分内容

- ▶ 第一部分：源程序及其代码

- ▶ 第二部分：各种标识符

- 错误Error：比较严重的语法错误

- 警告Warning：不太关键的语法错误



# 调试程序

- WinDbg是微软提供的Windows调试程序
- WinDbg支持源程序级调试，但汇编、连接时要加入参数

▶ 汇编时用“/Zi”（大写Z、小写i）参数

BIN\ML /c /coff /F1 /Zi eg0101.asm

▶ 连接时用“/debug”参数

BIN\LINK32 /subsystem:console /debug eg0101.obj



# 快速开发的批处理文件MAKE32.BAT

**@echo off**

**BIN\ML /c /coff /FI /Zi %1.asm**

**if errorlevel 1 goto terminate**

**BIN\LINK32 /subsystem:console /debug %1.obj**

**if errorlevel 1 goto terminate**

**DIR %1.\***

**:terminate**

**@echo on**

输入创建命令，生成可执行文件

D:\MASM>make32 eg0101

**温馨提示：** 无需输入源程序文件扩展名.ASM





# 快速开发过程

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
<C> 版权所有 1985-2001 Microsoft Corp.

D:\MASM>make32 eg0101
Microsoft (R) Macro Assembler Version 6.15.8803
Copyright (C) Microsoft Corp 1981-2000. All rights reserved.

Assembling: eg0101.asm
Microsoft (R) Incremental Linker Version 6.00.8168
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

驱动器 D 中的卷没有标签。
卷的序列号是 4D14-0C23

D:\MASM 的目录

2010-12-06 16:15
2010-12-06 17:13
2010-12-06 17:13          5,744 eg0101.lst
2010-12-06 17:13        20,388 eg0101.ilnk
2010-12-06 17:13        32,803 eg0101.exe
2010-12-06 17:13        74,752 eg0101.pdb
          6 个文件          135,602 字节
          0 个目录 58,760,757,248 可用字节

D:\MASM>eg0101
Hello, Assembly!

D:\MASM>
```

- ① 进入MASM目录：双击文件WIN32.BAT
- ② 生成可执行文件：make32 eg0101