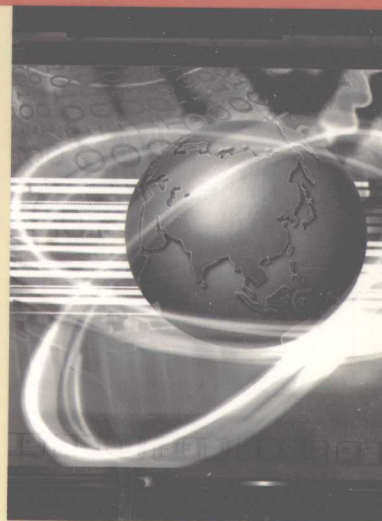




普通高等教育“十五”国家级规划教材配套教材

80X86

Assembly Language Programming



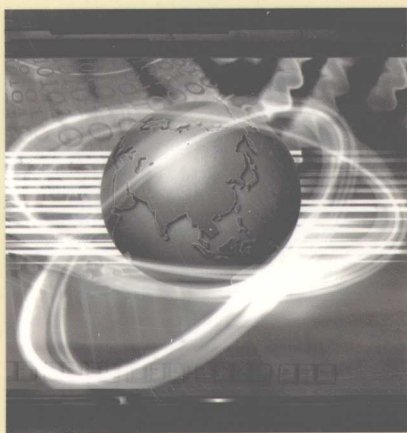
80X86

汇编语言程序设计上机指南

许向阳 编著

华中科技大学出版社
<http://www.hustp.com>

策划编辑 沈旭日
责任编辑 沈旭日



ISBN 978-7-5609-4000-7



9 787560 940007 >

定价: 23.80元 (含1CD)

TP313
108

TP313
108



普通高等教育“十五”国家级规划教材



80X86
Assembly Language Programming

80X86 汇编语言程序设计上机指南

许向阳 编著

责任编辑：林五英

80X86 汇编语言

责任编辑：林五英

华中科技大学出版社

华中科技大学出版社

ISBN 978-7-5693-4000-7
定价：23.80元

华中科技大学出版社

图书在版编目(CIP)数据

80X86汇编语言程序设计上机指南/许向阳 编著. —武汉:华中科技大学出版社,
2007年4月

ISBN 978-7-5609-4000-7

I. 8… II. 许… III. 汇编语言-程序设计-高等学校-教学参考资料 IV. TP313

中国版本图书馆CIP数据核字(2006)第151847号

80X86 汇编语言程序设计上机指南

许向阳 编著

责任编辑:沈旭日

封面设计:潘群

责任校对:代晓莺

责任监印:张正林

出版发行:华中科技大学出版社

武昌喻家山 邮编:430074 电话:(027)87557437

录排:华中科技大学惠友文印中心

印刷:湖北恒泰印务有限公司

开本:787mm×1092mm 1/16

印张:14.75

字数:323 000

版次:2007年4月第1版

印次:2007年4月第1次印刷

定价:23.80元(含1 CD)

ISBN 978-7-5609-4000-7/TP·631

(本书若有印装质量问题,请向出版社发行部调换)

内 容 简 介

本书为“80X86 汇编语言程序设计”课程的配套教材。

全书分为两个部分,共 11 章。第 1 章至第 6 章为第一部分,介绍实方式环境下 16 位汇编语言程序设计的上机实践。主要内容包括 MASM 和 TASM 的上机操作过程、常见汇编和连接错误、调试器 TD 的使用方法、子程序库的应用,以及高级的汇编语言程序设计技术。第 7 章至第 11 章为第二部分,介绍 Windows 环境下 32 位汇编语言程序的上机实践,包括 MASM32 软件包、调试器 W32Dasm 和 SoftICE 的使用方法、Win32 程序的开发实例、C 语言和汇编语言程序的连接。

本书内容丰富,图文并茂,语言精练易懂,大量的程序实例扩展了教科书的内容,可供各类高等学校计算机及相关专业作为辅导教材,亦可供具有汇编语言程序设计基本理论知识的广大工程技术人员和其他读者自学、参考。

前 言

汇编语言是计算机提供给用户的最快而又最有效的语言,也是能够利用计算机所有硬件特性并能直接控制硬件的唯一语言。“汇编语言程序设计”是计算机类专业的重要专业基础课,是从事计算机研究与应用,特别是软件研究的基础,是计算机专业人员必须接受的最重要的专业基础训练之一。

“汇编语言程序设计”是一门实践性很强的课程。因此,在学习汇编语言程序设计的过
程中,只有多阅读程序、多编写程序、多上机,才能真正掌握程序设计的方法和技巧。目前,
最为广泛使用的 PC 机皆以 Intel 的 80X86 及其兼容的微处理器为 CPU,运行环境为 Win-
dows 和 DOS。本书的目的是帮助具有汇编语言程序设计基本理论知识的读者更好地领会
和掌握汇编语言程序设计知识,掌握上机的操作方法,熟练使用常用的调试工具,提高程序
阅读和编写能力。

本书在内容的组织上,力求由浅入深、循序渐进。对于初次接触汇编语言上机操作者,
通过自学完全可以掌握;对于有一定经验的实践者,可以学到技巧较高的实用操作方法;而
对于已掌握教材内容的读者,可以拓宽知识面、开阔视野、增长灵活运用能力。在内容的
选取上,力求新颖丰富,知识面广,尽可能地避免和教材内容重复,因而重点介绍了 Win32 程
序设计,介绍了程序反汇编和逆向分析技术。在内容的表述上,力求通俗易懂、图文并茂、便
于自学。

全书分为两个部分,共 11 章。第 1 章至第 6 章为第一部分,介绍 DOS 环境下汇编语言
程序设计的上机实践。第 7 章至第 11 章为第二部分,介绍 Windows 环境下汇编语言程序
的开发和上机实践。其中,第 1 章介绍上机的基本操作步骤,包括上机的工作环境、汇编源
程序的编辑、汇编和连接;第 2 章介绍常见的汇编和连接错误;第 3 章详细介绍调试器 TD
的使用方法;第 4 章介绍 TASM 软件包及带符号的程序调试;第 5 章介绍多模块程序设计
方法,重点介绍一个共享子程序库 STDLIB;第 6 章给出一些实方式下程序实例,涉及命令
行的读取、输入、输出及中断程序设计、文件操作等。第 7 章介绍 MASM32 软件包及 Win32
程序的编译、链接方法;第 8 章给出一个典型的 Windows 环境下的文本编辑器的开发过程,
涉及 Windows 窗口、对话框、文本编辑控件、菜单、图标、工具栏、状态栏的资源编辑和编程;
第 9 章介绍调试工具 W32Dasm 的使用方法;第 10 章介绍符号调试工具 SoftICE;第 11 章
介绍汇编语言程序和 C 语言程序的连接方法。在主要章节后附有一定的上机操作实践习
题,这些习题有助于读者掌握书中介绍的工具。通过阅读程序,可以进一步学习编程规律和
技巧。

为了便于读者学习,本书附带了学习光盘,包括多种开发包和本书涉及的程序实例,还有一些未在书中介绍的程序实例,其目的是增大读者的程序阅读量,开阔眼界。

本书由许向阳编著。在编写本书的过程中得到了华中科技大学计算机学院、“汇编语言程序设计课程”课程组,特别是王元珍教授、曹忠升副教授的热情帮助和支持,得到了华中科技大学出版社有关领导和有关编辑的关心和帮助,在此一并表示衷心感谢。

由于作者水平有限,书中不妥或错误之处在所难免,殷切希望广大读者不吝批评指正。

作者

2006年12月于华中科技大学(武汉)

目 录

第 1 章 实方式上机入门	(1)
1.1 生成第一个程序 DEMO	(1)
1.1.1 建立工作环境	(1)
1.1.2 DEMO 的编辑	(1)
1.1.3 DEMO 的汇编	(3)
1.1.4 DEMO 的连接	(5)
1.1.5 DEMO 的运行	(6)
1.2 生成实方式程序的过程	(6)
1.3 运行环境	(7)
1.4 汇编和连接的高级操作	(8)
1.4.1 MASM 命令及参数	(8)
1.4.2 ML 命令和参数	(9)
1.4.3 LINK 命令及参数	(11)
1.5 建立更好的工作环境	(12)
第 2 章 常见的汇编和连接错误	(17)
2.1 汇编时的常见现象	(17)
2.1.1 汇编时常见的异常现象	(17)
2.1.2 汇编成功的检验	(19)
2.2 常见的汇编错误及其分析	(19)
2.2.1 程序中有不恰当的中文符号	(19)
2.2.2 段定义伪指令错误	(21)
2.2.3 指令错误	(22)
2.2.4 程序结构错误	(25)
2.2.5 变量定义错误	(26)
2.2.6 连接错误	(27)
2.3 汇编查错技巧	(27)
第 3 章 实方式程序调试器 TD	(30)
3.1 TD 的启动和退出	(30)
3.1.1 启动 TD	(30)
3.1.2 退出 TD	(31)
3.2 TD 的用户界面	(31)
3.3 DEMO 的调试	(34)
3.3.1 在数据区观察程序的机器码	(34)
3.3.2 观察源程序中数据段的数据	(35)
3.3.3 程序的执行及结果的查看	(36)

3.3.4	程序的再次执行及断点设置	(38)
3.4	载入新程序及执行程序的修改	(39)
3.4.1	打开一个文件	(40)
3.4.2	改变文件目录	(41)
3.4.3	修改指令代码	(41)
3.4.4	修改程序中的数据	(42)
3.5	有子程序的程序调试	(43)
3.5.1	观察以双字形式显示的数据段	(45)
3.5.2	直接运行到 CALL 指令处暂停	(46)
3.5.3	跟踪到子程序中	(47)
3.6	中断处理程序的调试	(48)
3.6.1	中断处理程序的入口地址	(49)
3.6.2	中断处理程序的显示	(50)
3.6.3	进入软中断的处理程序	(50)
3.7	代码区和数据区的操作菜单	(51)
3.7.1	代码区操作菜单	(51)
3.7.2	数据区操作菜单	(52)
3.7.3	TD 中数据输入说明	(53)
第 4 章	带符号的程序调试	(62)
4.1	TASM 的安装	(62)
4.2	生成有调试信息的文件	(64)
4.3	带符号的程序调试	(70)
4.3.1	启动程序调试	(70)
4.3.2	打开 CPU 窗口	(71)
4.3.3	改变 CPU 窗口中代码的显示模式	(72)
4.3.4	窗口的打开、关闭及大小、位置调整	(72)
4.3.5	Watches 窗口操作	(73)
4.3.6	带条件的断点设置	(74)
第 5 章	多模块程序的运行及子程序库	(78)
5.1	宏库的建立和使用	(78)
5.2	多模块程序的开发	(80)
5.3	子程序库的建立和使用	(84)
第 6 章	实方式下汇编程序实例及课程设计	(92)
6.1	命令参数行的获取	(92)
6.1.1	EXE 程序的参数获取	(92)
6.1.2	COM 程序的参数获取	(93)
6.2	乐曲演奏程序	(95)
6.2.1	扬声器的驱动方式	(95)
6.2.2	乐曲演奏程序	(98)
6.3	文件管理	(101)

6.3.1	文件读取程序	(101)
6.3.2	文件管理功能调用说明	(103)
6.4	课程设计	(105)
第7章 Win32 编程环境		(111)
7.1	MASM32 软件包简介	(111)
7.1.1	MASM 系列编译器介绍	(111)
7.1.2	MASM32 软件包	(112)
7.2	MASM32 软件包安装	(112)
7.3	使用 QEDITOR	(115)
7.3.1	首次使用 QEDITOR	(115)
7.3.2	QEDITOR 揭密	(117)
7.4	生成 Win32 程序的过程	(120)
7.4.1	汇编源文件和资源脚本的编辑	(120)
7.4.2	汇编源文件的编译	(120)
7.4.3	资源脚本的编译	(123)
7.4.4	执行文件的生成	(123)
7.4.5	建立更好的环境	(127)
7.5	nmake 工具	(128)
7.5.1	首次使用 nmake 工具	(128)
7.5.2	描述文件的语法	(129)
7.5.3	nmake 的高级用法	(132)
第8章 文本编辑器开发		(134)
8.1	创建一个窗口程序	(134)
8.1.1	创建一个窗口	(134)
8.1.2	Windows 消息的处理过程	(136)
8.2	增加 RichEdit 控件	(138)
8.3	创建图标	(139)
8.3.1	在程序中加载图标	(139)
8.3.2	用 VC++ 制作图标	(141)
8.4	制作与加载菜单	(143)
8.4.1	用文本编辑器制作菜单	(143)
8.4.2	用 VC++ 制作菜单	(145)
8.5	打开与保存文件	(148)
8.5.1	打开文件的步骤	(148)
8.5.2	打开文件程序实例	(149)
8.5.3	保存文件及文件另存为	(152)
8.5.4	退出系统及消息响应	(154)
8.6	RichEdit 控件的控制消息	(155)
8.7	创建工具栏	(157)
8.7.1	使用通用位图创建工具栏	(157)

8.7.2	创建自定义位图的工具栏	(159)
8.7.3	使用消息创建工具栏	(162)
8.8	增加状态栏	(164)
8.9	查找字符串	(166)
8.9.1	使用通用“查找”对话框	(166)
8.9.2	使用自定义对话框	(169)
8.10	编辑器优化	(172)
第9章	反汇编及调试工具 W32Dasm	(179)
9.1	W32Dasm 软件包的组成及启动	(179)
9.2	W32Dasm 的程序浏览	(180)
9.3	程序的动态调试	(186)
9.3.1	程序调试的启动	(186)
9.3.2	断点的设置和取消	(189)
9.3.3	存储单元中值的观察	(190)
9.3.4	数据的修改	(191)
9.3.5	显示 EIP 指示的指令	(192)
9.4	WinAPI 的细节信息	(192)
9.5	程序的修改及反汇编代码的保存	(194)
9.6	进程调试及程序暴力破解示例	(196)
第10章	调试工具 SoftICE	(199)
10.1	SoftICE 简介	(199)
10.1.1	SoftICE 调试器	(199)
10.1.2	符号载入工具 Symbol Loader	(200)
10.2	SoftICE 的安装	(200)
10.3	SoftICE 启动	(202)
10.4	SoftICE 符号调试	(205)
10.4.1	建立含调试信息的执行文件	(205)
10.4.2	装入 richedit11 程序	(206)
10.4.3	简单的调试	(208)
10.5	设置断点	(210)
10.5.1	执行断点	(210)
10.5.2	内存断点	(213)
10.5.3	其他类型的断点	(214)
10.6	SoftICE 的其他信息	(215)
第11章	汇编语言程序与 C 语言程序的连接	(216)
11.1	内嵌汇编	(216)
11.1.1	内嵌汇编示例及优势分析	(216)
11.1.2	内嵌汇编语法及用法示例	(218)
11.2	VC++ 调用汇编语言子程序	(221)
参考文献		(225)

第 1 章

入门方式上机

本章通过一个运行程序的建立过程介绍上机的基本操作,包括上机的工作环境、汇编源程序的编辑、汇编和连接;然后,对汇编和连接命令的参数进行详细的解释,并介绍建立一个良好工作环境的方法。

1.1 生成第一个程序 DEMO

1.1.1 建立工作环境

本书中采用的汇编程序是 Microsoft 公司提供的 MASM6.0,并假设 masm6 中的文件存放在 D:\masm6 目录下。当然,masm6 也可以存放在其他目录下,但要注意将下面示例中的文件路径同时改掉。一般情况下,masm6 无需安装,程序可以直接运行。

若要确认 D:\masm6 是否包含了汇编、连接和调试时需要的程序,则可以打开资源管理器进行查看。

1. 宏汇编程序

masm6 下的宏汇编程序是 Microsoft 公司提供的 MASM 6.0 程序,其主要内容包括: MASM.EXE、ML.EXE 和 ML.ERR 等。

2. 连接器

连接器文件为 LINK.EXE,这也是 MASM 的配套软件。

3. 调试器

调试器 TD.EXE 是 Borland 公司的产品,用于调试实方式下的 16 位段程序。该软件一般出现在 TASM 软件包中。

1.1.2 DEMO 的编辑

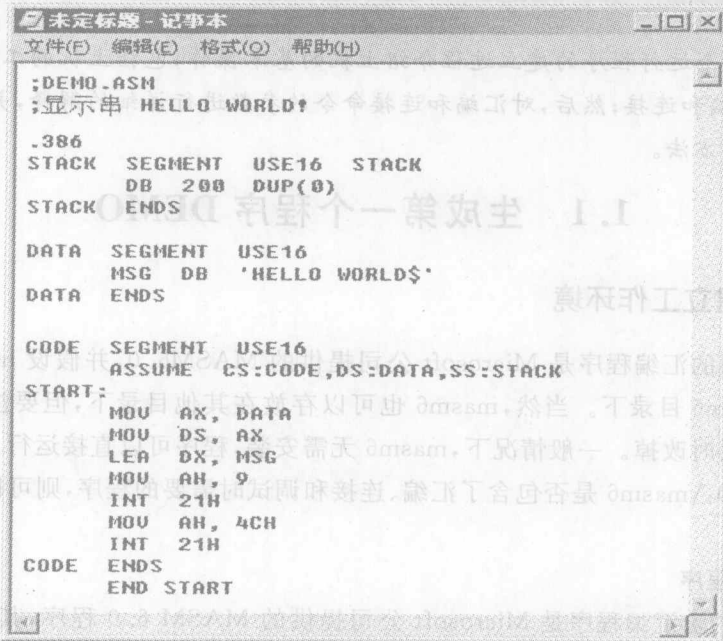
采用 Windows 系统自带的记事本 (Notepad.exe) 编辑汇编源程序。如图 1.1 所示,单



图 1.1 启动记事本程序

击“开始”，将光标移至“程序”，在出现程序菜单后，将光标移至“附件”，再移到“记事本”（注：本书给出的操作界面都是 Windows 2000 下的，若读者使用的是不同的操作系统，则界面可能会有所不同）。单击“记事本”，将出现“记事本”窗口。

“记事本”是一个全屏幕编辑器，可以使用鼠标、键盘进行编辑操作。图 1.2 给出了完整的 DEMO.ASM 源程序。



```

;DEMO.ASM
;显示串 HELLO WORLD!

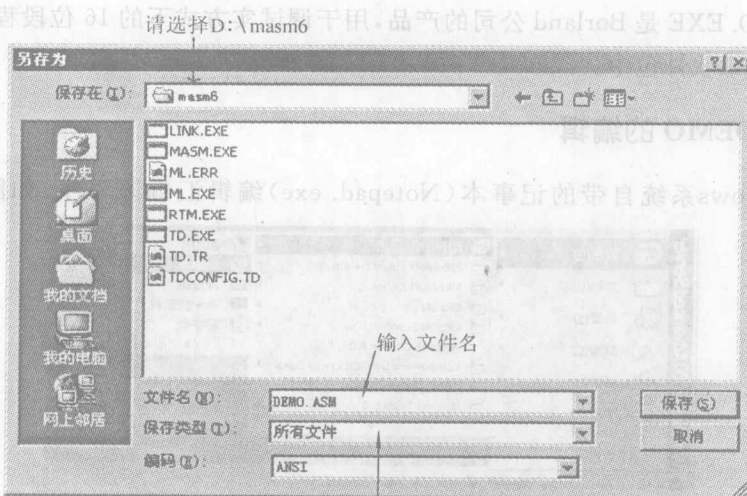
.386
STACK SEGMENT USE16 STACK
DB 200 DUP(0)
STACK ENDS

DATA SEGMENT USE16
MSG DB 'HELLO WORLD$'
DATA ENDS

CODE SEGMENT USE16
ASSUME CS:CODE,DS:DATA,SS:STACK
START:
MOV AX, DATA
MOV DS, AX
LEA DX, MSG
MOV AH, 9
INT 21H
MOV AH, 4CH
INT 21H
CODE ENDS
END START
  
```

图 1.2 记事本及 DEMO.ASM 源程序

在输入完成后，单击“记事本”上的“文件”菜单，在弹出的下拉式菜单上单击“保存”菜单项，将出现如图 1.3 所示的界面。



默认的是“文本文档 (*.TXT)”，此处请换成“所有文件”

图 1.3 源程序的保存

在保存窗口中,应注意以下几个问题:

- 保存文件的位置应在 D:\masm6 中;
- 文件名为 DEMO.ASM;
- 保存类型为“所有文件”。

说明 如果保存类型为“文本文档(*.TXT)”,则保存的文件最后的扩展名为“.TXT”,也就是说,若在文件名输入栏中的名字是“DEMO.ASM”,则实际保存的文件名将是“DEMO.ASM.TXT”;若保存类型为“所有文件”,则不会在输入的文件名后加“.TXT”。

最后,可以在资源管理器中看到在 D:\masm6 下有 DEMO.ASM 文件,其文件类型为“ASM 文件”。

1.1.3 DEMO 的汇编

首先,打开“命令提示符”窗口。在“记事本”窗口的下方有一个“命令提示符”菜单项,单击它,将在屏幕上出现一个“命令提示符”窗口。打开“命令提示符”窗口的另一种方法是:先单击“开始”,再单击“运行”菜单项,在出现的图 1.4 所示的录入框中输入“cmd”后按回车键。

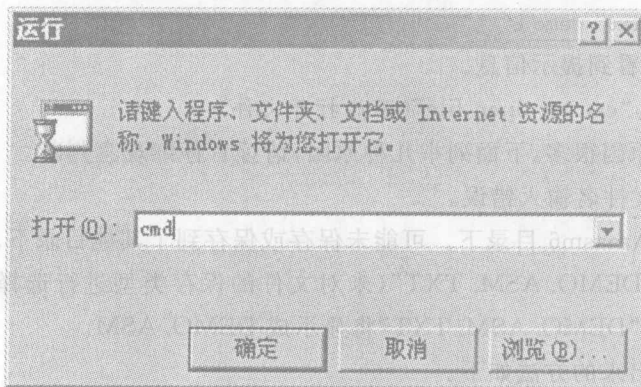


图 1.4 Windows 运行程序的一种方法

然后,在“命令提示符”窗口中依次执行如下操作(用户只需输入带下划线的部分,↵表示回车,下同)。

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

```
D:\> cd masm6↵
```

```
D:\masm6> masm demo↵
```

其中,有下划线的部分就是输入的命令。

注意 命令中可以使用大写字母、小写字母或者混用,其结果是相同的。

上述操作的结果如图 1.5 所示。

如果没有什么异常情况发生,就可以直接进入 1.1.4 小节所介绍的 DEMO 的连接了。

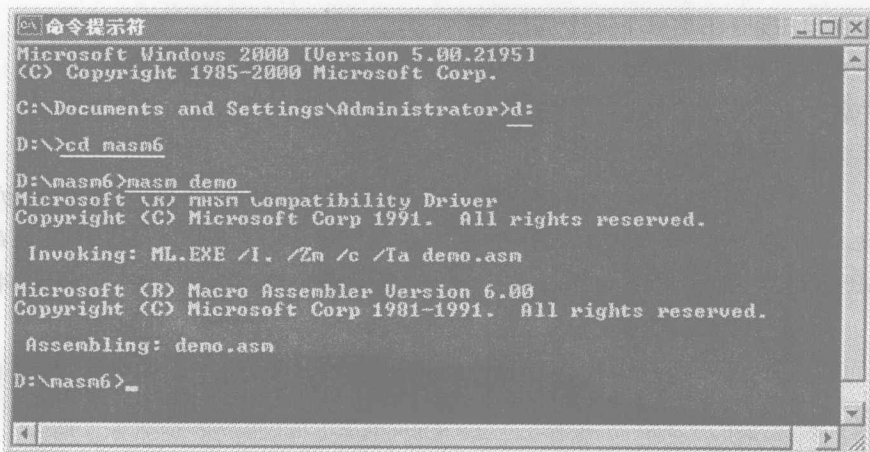


图 1.5 DEMO 的汇编

汇编过程中可能出现的异常情况如下。

(1) 无任何提示信息

无任何提示信息,并不是表示汇编已成功了,而是表示可能有错误,但未显示出来。这时,可按组合键 Alt+Enter,将“命令提示符”窗口全屏化,之后再执行如下命令:

```
D:\masm6> masm demo
```

此时,应该可以看到提示信息。

(2) 有提示信息“cannot open file”(不能打开文件)

出现该问题的原因很多,下面列举几种原因,请读者仔细观察判断。

- 命令行上的文件名输入错误。
- 文件不在 D:\masm6 目录下。可能未保存或保存到了其他目录下。
- 文件被存为“DEMO. ASM. TXT”(未对文件的保存类型进行选择)。由于文件的扩展名可以被隐藏,故“DEMO. ASM. TXT”将显示成 DEMO. ASM。

将扩展名显示出来的方法如下。

打开资源管理器,单击“工具/文件夹选项”,出现如图 1.6 所示的界面。在“查看”卡片下单击“隐藏已知文件类型的扩展名”,将其前面的“√”去掉。之后,单击“确定”按钮。

此时,再观察 D:\masm6 下的文件名是否为 DEMO. ASM. TXT,若是,则需修改。操作方法是:右击文件名,在弹出的菜单上选择“重命名”,之后输入新的文件名。

(3) 指出某一行有错误

在程序输入过程中出现了错误时,需要修改 DEMO. ASM。操作方法是:在资源管理器中显示出 masm6 目录,然后双击“DEMO. ASM”,选择使用记事本(Notepad)打开扩展名为“. ASM”的文件。在打开该文件后,进行修改。

注意 文件修改完成后,一定要保存。

有关汇编错误的更多解释将在第 2 章中介绍。

在修改并保存源程序后,可以不关闭 Notepad,而是直接切换到“命令提示符”窗口,对 DEMO. ASM 进行汇编。先修改源程序然后汇编的过程也许有几个反复。

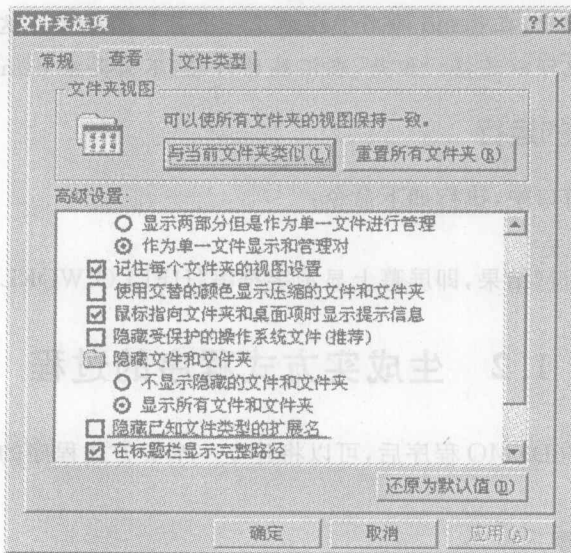


图 1.6 文件夹选项窗口

在对 DEMO.ASM 汇编成功后,在 D:\masm6 目录下可以看到已生成了一个 DEMO.OBJ 文件,并且其字节数不是 0。

(4) 与 MASM 有关的错误

检查汇编所需要的软件是否都已在 D:\masm6 目录下。如果存在问题,则可以将这些文件重新拷贝一次。

1.1.4 DEMO 的连接

汇编成功后,可在图 1.5 所示的窗口中执行如下命令:

```
D:\masm6> link demo;
```

将出现如图 1.7 所示的界面。

```
命令提示符
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>d:
D:\>cd masm6
D:\masm6>masm demo
Microsoft (R) MASM Compatibility Driver
Copyright (C) Microsoft Corp 1991. All rights reserved.

Invoking: ML.EXE /I. /Zm /c /Ta demo.asm
Microsoft (R) Macro Assembler Version 6.00
Copyright (C) Microsoft Corp 1981-1991. All rights reserved.

Assembling: demo.asm
D:\masm6>link demo;
Microsoft (R) Segmented Executable Linker Version 5.20.034 May 24 1991
Copyright (C) Microsoft Corp 1984-1991. All rights reserved.
D:\masm6>
```

图 1.7 DEMO 的连接

注意 在连接命令中,在 demo 的名字后加了一个英文的分号。这样,在连接的时候,不需用户输入其他信息就可以连接。但是,在汇编的时候,不需要在 demo 后加英文分号。

1.1.5 DEMO 的运行

在图 1.7 所示的窗口中,执行如下命令:

```
D:\masm6> demo ↵
```

应该可以看到程序的运行结果,即屏幕上显示字符串“HELLO WORLD”。

1.2 生成实方式程序的过程

生成 1.1 节所述的 DEMO 程序后,可以将建立一个实方式程序的过程进一步明确为以下几个步骤。

1. 建立汇编源程序

用某一种编辑程序建立汇编源程序。建立汇编源程序后,应注意将其保存到磁盘上。一种简单的方法是将源程序保存到 MASM.EXE 所在的目录中。

汇编源程序文件的扩展名一般取为“.ASM”。

2. 汇编源文件,生成目标文件

汇编源文件的过程就是汇编,其主要功能是检查程序有无语法错误,并且在程序无误时,生成目标文件(扩展名为“.OBJ”)。

在汇编源文件过程中出现错误时,要返回第 1 步,即建立汇编源程序,并对源程序进行修改。在修改完成后,要保存文件。之后,再次对源文件进行汇编。该过程也许要进行多次,直到无汇编错误并生成目标文件为止。

一些常见的汇编错误将在第 2 章介绍。熟悉这些错误,可以提高找出语法错误的能力。

3. 连接目标文件

连接目标文件,建立可执行文件(扩展名为“.EXE”)。

在连接多模块程序(即多个文件),或者连接某些库时,还有可能产生错误。例如,在一个模块中引用了一个变量,而在其他模块中找不到定义,等等。此时可能要返回第 1 步,进行适当修改,然后再进行第 2、3 步的操作。

一些常见的连接错误将在第 2 章介绍。多模块程序的连接将在第 5 章中介绍。

4. 运行、调试程序

在生成可执行文件后,要运行该程序,看其是否能完成预定的功能。测试时应尽可能多地选用各方面都具有代表性的数据。

在程序运行异常时,需要对程序进行调试,找出问题。发现错误后,还要对源程序进行修改,然后再依次执行第 2、3、4 步的操作。该过程也许要反复进行,直到确认程序无误为止。详细的调试程序的方法,将在第 3 章介绍。