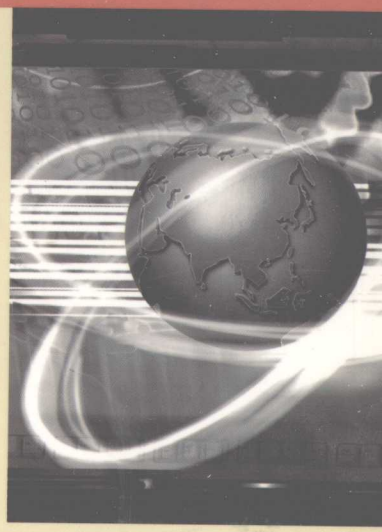
普通高等教育“十五”国家级规划教材配套教材

精品课程

80X86
Assembly Language Programming

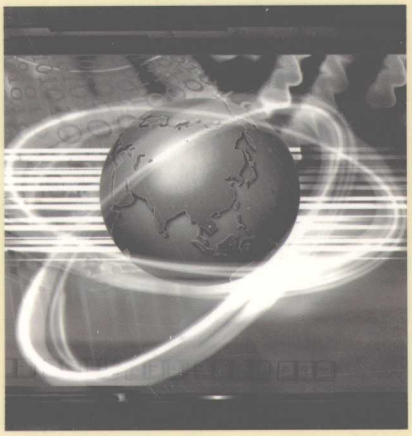


80X86
汇编语言程序设计上机指南

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

普通高等教育“十五”国家级规划教材

精品课程

附光盘

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

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。

试读结束：需要全本请在线购买： www.ertongbook.com

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 Windows 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、增长灵活运用的能力。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

试读结束：需要全本请在线购买： www.ertongbook.com

第1章 实方式上机入门

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。

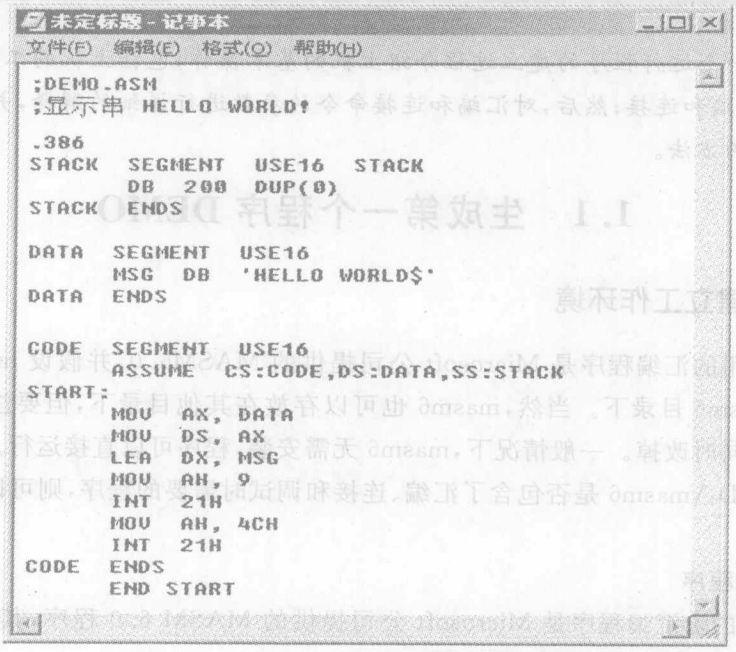


图 1.2 记事本及 DEMO.ASM 源程序

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。

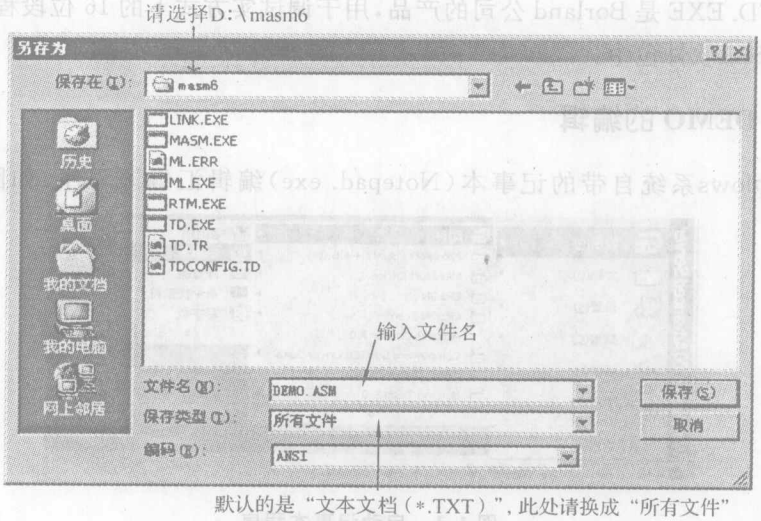


图 1.3 源程序的保存

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。

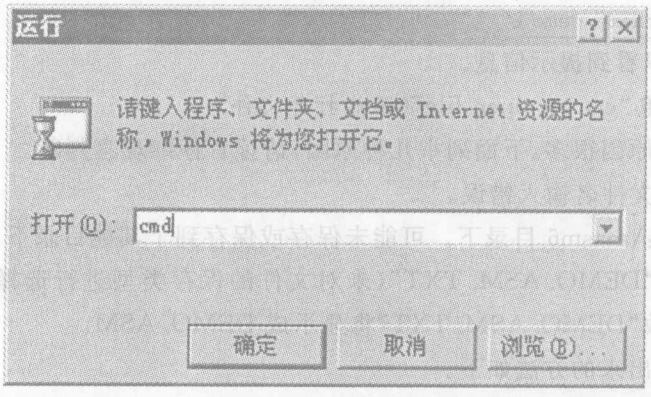


图 1.4 Windows 运行程序的一种方法

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。

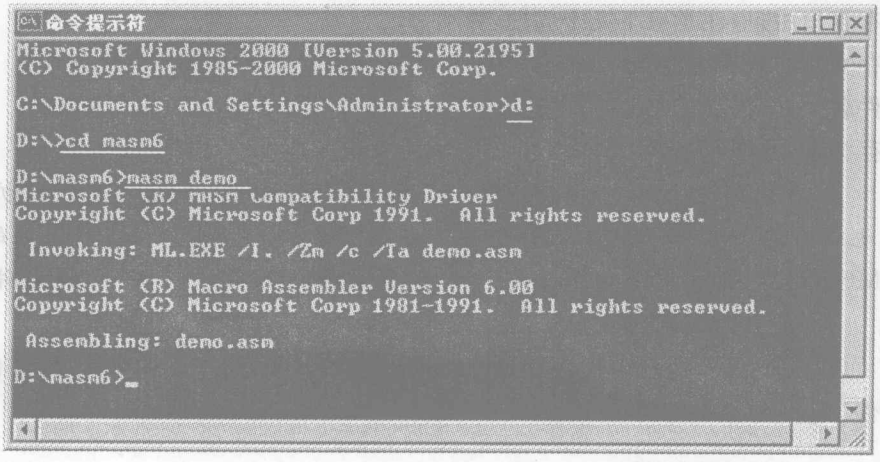


图 1.5 DEMO 的汇编

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。

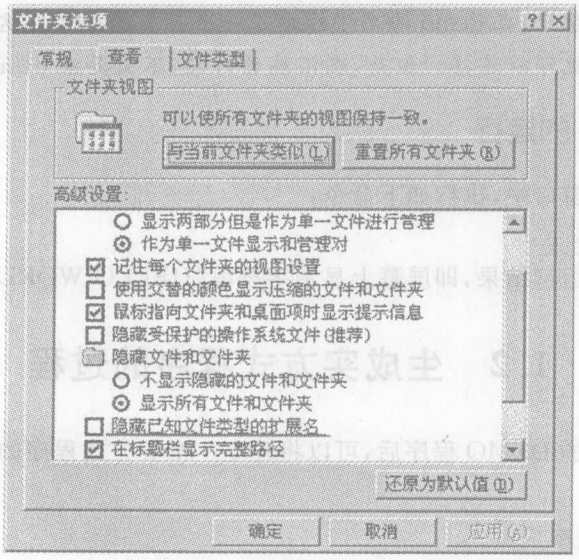


图 1.6　文件夹选项窗口

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。

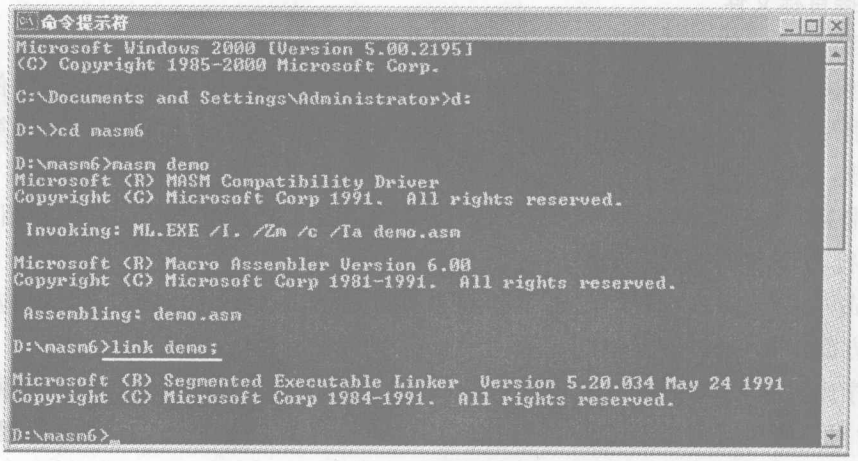


图 1.7　DEMO 的连接

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。

试读结束：需要全本请在线购买： www.ertongbook.com