

8086 / 386 系列 汇编语言程序设计

王 方 新

北京邮电学院出版社

8086/386 系 列

汇 编 语 言 程 序 设 计

王 方 新

北 京 邮 电 学 院 出 版 社

(京)新登字 162 号

8086/386 系列

汇编语言程序设计

编 者 王方新

责任编辑 周 明

*

北京邮电学院出版社出版

新华书店北京发行所发行 各地新华书店经售

北京建新印刷厂印刷

*

850×1168 毫米 1/32 印张 13.875 字数 372 千字

1994 年 6 月第一版 1994 年 6 月第一次印刷

印数：1—3000 册

ISBN 7-5635-0167-3/TP·16 定价：10.10 元

图书在版编目 (CIP) 数据

8086/386 系列汇编语言程序设计/王方新编. -北京: 北京邮电学院出版社, 1994

ISBN 7-5635-0167-3

I. 80… II. 王… III. 汇编语言-程序设计 N. TP313

中国版本图书馆 CIP 数据核字 (94) 第 09032 号

内 容 简 介

本书作为计算机汇编语言程序设计课程的教材,是根据邮电院校八五教材规划、在已使用四年讲义的基础上修改、完善而成的。全书分为七章,以 8086/386 汇编语言为背景,分别介绍了 8086/286 以及 386 微计算机系统结构、指令系统、宏汇编语言 MASM、程序设计方法、中断与 DOS 调用、输入输出程序设计及 286/386 保护模式程序设计。本书在编写中避免了手册式的繁琐叙述,突出重点,深入浅出,循序渐进。例题兼顾了语法规则和程序设计方法,并把程序设计方法放在主要地位。例题涉及常用算法并结合实时控制、通信和信号处理应用。各章都配备一定数量的习题以及实验上机题。在附录部分介绍了汇编连接工具 MASM, LIB, LINK, 调试工具 DEBUG, CodeView 以及 DOS 系统功能调用表, 8086/88/286 指令代码表等。本书易于入门和自学,除可用作高校“汇编语言程序设计”课程的教材外,也可供计算机、通信、自控、电子类工程技术人员学习参考。

编者的话

本书是根据邮电高等院校计算机类专业教学指导委员会制定的大纲和要求编写的,并由教学指导委员会推荐作为邮电高校计算机专业“汇编语言程序设计”教材。

从1987年起,本书一直作为院内讲义用于对本(专)科及部分专业研究生讲授8086/286汇编语言程序设计,并经多次修改。考虑到学生上机条件的不断改善,还介绍了386实模式程序设计和286/386保护模式程序设计。在编写及修改中力求突出重点,避免手册式的繁琐叙述,强调以课堂对话和较多的例题来说明问题,以便于学生自学。在处理语句规则和程序设计的不关系方面,将程序设计思想和方法放在主要的地位。另外,本书还介绍了DOS中断调用和系统功能调用的实际应用以及输入输出程序设计的一般方法。因此,本书不仅可以用作教材,也可供计算机、通信、电子和自控类专业工作者参考。

为便于联系应用实际,本书选用最为流行的IBM PC系列机8086/286/386汇编语言MS-MASM为蓝本。多数程序进行过上机调试,例题中适当考虑了实际的控制和通信应用。习题则考虑了学生的实际情况,既易于入门又有一定深度,每章习题后还给出了实验上机题。目录中标有“*”号的章节可根据情况少讲或不讲,留给学生参考。

本书的出版得到了邮电部计算机类专业教学指导委员会的热忱支持和帮助,教指委的老师们审阅了全书并提出了宝贵的修改意见。在本书编写和修改过程中,重庆邮电学院屠善濂副教授、北京邮电学院李怀诚副教授、重庆大学李朴教授、西安邮电学院赵亚

婉副教授以及重庆邮电学院汪林林副教授、裘湘惠副教授、曾省三高级工程师、邓亚平副教授等提出过很好的意见,高扬同志协助做了很多工作。魏红同志,以及莫小青、田航、罗俊春等同志参与了资料收集和整理,计算机系学生协助录入了部分章节。北京邮电学院出版社周明老师作为责任编辑,为本书的修改和完善做出了卓有成效的工作。对于上述老师和同志们的支持,编者谨表示真挚的感谢。

由于编者水平及条件限制,书中难免有谬误之处,恳请读者指正。

编 者

1993年7月于重庆邮电学院

目 录

编者的话..... (1)

绪论..... (1)

第一章 Intel 8086 体系结构

§ 1-1 微型计算机系统 (6)

§ 1-2 8086 CPU (9)

1-2-1 8086 CPU (9)

1-2-2 寄存器组 (11)

1-2-3 CPU 执行指令的过程 (12)

1-2-4 总线接口单元与执行单元 (15)

1-2-5 8086 系统总线结构 (16)

§ 1-3 段寄存器 (17)

§ 1-4 标志寄存器 FLAG (19)

1-4-1 控制标志 (19)

1-4-2 状态标志 (20)

§ 1-5 堆栈 (22)

* § 1-6 80286/386 (24)

1-6-1 80286 (24)

1-6-2 80386 (26)

1-6-3 80386 的寄存器组 (27)

* § 1-7 80486/Pentium (29)

1-7-1 80486	(29)
1-7-2 Pentium	(29)
习题一	(30)
实验题一	(31)

第二章 指令系统

§ 2-1 寻址方式	(32)
2-1-1 寻址方式	(32)
2-1-2 寻址方式的比较	(38)
* § 2-2 80386 寻址方式	(38)
§ 2-3 指令系统	(40)
2-3-1 数传指令	(40)
2-3-2 算术运算指令	(44)
2-3-3 逻辑运算指令	(45)
2-3-4 移位指令	(47)
2-3-5 数据串操作指令	(49)
2-3-6 转移指令	(54)
2-3-7 处理器控制指令	(55)
§ 2-4 80286 的指令扩充	(56)
§ 2-5 指令代码格式	(56)
习题二	(59)
实验题二	(61)

第三章 汇编语言

§ 3-1 汇编语言语句	(62)
3-1-1 汇编语言语句	(64)
3-1-2 参数	(65)
3-1-3 标识符 (Identifier)	(67)

3-1-4	运算和操作符	(67)
§ 3-2	常量	(68)
3-2-1	常量的定义	(68)
3-2-2	串常量 (正文宏)	(69)
§ 3-3	变量	(70)
3-3-1	变量的定义	(70)
3-3-2	变量的属性	(72)
3-3-3	变量的使用	(74)
§ 3-4	标号	(76)
3-4-1	标号的类型与属性	(76)
3-4-2	标号的定义	(77)
§ 3-5	TYPE, SIZE 与 LENGTH	(79)
§ 3-6	类型的改变与指定	(79)
3-6-1	PTR 运算符	(80)
3-6-2	THIS 运算符	(81)
3-6-3	LABEL 运算符	(81)
§ 3-7	汇编语言程序结构	(82)
3-7-1	模块 (Module) 结构	(82)
3-7-2	段 (Segment)	(84)
3-7-3	过程 (Procedure)	(91)
3-7-4	群 (Group)	(92)
§ 3-8	简化的段定义	(93)
§ 3-9	结构与记录	(96)
3-9-1	结构 (Structure)	(96)
3-9-2	记录	(98)
§ 3-10	条件汇编	(100)
§ 3-11	宏指令语句	(101)
3-11-1	宏操作伪指令	(102)

3-11-2	重复块定义伪指令	(104)
3-11-3	符号处理与 LOCAL 伪指令	(105)
3-11-4	嵌套宏定义	(106)
3-11-5	嵌套宏调用	(107)
3-11-6	重复宏定义	(109)
3-11-7	宏定义库的使用——INCLUDE 伪指令	(109)
§ 3-12	汇编过程与汇编程序	(111)
§ 3-13	连接程序	(119)
§ 3-14	汇编语言程序的运行环境	(121)
3-14-1	操作系统	(121)
3-14-2	DOS 的内部和外部命令	(122)
3-14-3	中断与系统功能调用	(123)
* § 3-15	EXE, COM 文件结构与程序段前缀 PSP	(126)
3-15-1	程序段前缀 PSP	(126)
3-15-2	EXE 文件结构	(128)
3-15-3	COM 文件	(130)
3-15-4	内存控制块与环境块	(132)
习题三		(132)
实验题三		(134)

第四章 程序设计方法

§ 4-1	顺序结构	(137)
4-1-1	简单数制变换	(137)
4-1-2	简单数码转换	(139)
4-1-3	重复宏定义和嵌套段定义在数码转换中的应用	(145)
§ 4-2	分支结构	(146)

4-2-1	无条件转移指令	(149)
4-2-2	条件转移指令	(152)
4-2-3	分支程序设计	(154)
4-2-4	多分支程序设计	(155)
§ 4-3	循环结构	(158)
4-3-1	循环指令 LOOP	(158)
4-3-2	多重循环	(161)
§ 4-4	子程序	(170)
4-4-1	子程序结构	(170)
4-4-2	调用指令 CALL	(171)
4-4-3	返回指令 RET	(172)
4-4-4	子程序库	(172)
4-4-5	参数的传递	(172)
4-4-6	嵌套	(174)
4-4-7	递归	(178)
§ 4-5	算术运算	(182)
4-5-1	十进制运算	(182)
4-5-2	乘法运算	(186)
4-5-3	除法运算	(190)
4-5-4	符号扩展指令	(192)
§ 4-6	浮点数运算	(193)
§ 4-7	可浮动程序与可再入程序	(197)
4-7-1	可浮动程序	(197)
4-7-2	可再入程序	(199)
* § 4-8	汇编语言子程序与高级语言的接口	(200)
4-8-1	模块之间的连接方式	(201)
4-8-2	参数传递方法	(202)
* § 4-9	386 实地址模式程序设计	(204)

4-9-1	386 的实地址模式	(204)
4-9-2	段字设置	(205)
4-9-3	386 的指令扩充	(206)
4-9-4	程序设计实例	(208)
习题四	(210)
实验题四	(212)

第五章 中断与 DOS 调用的程序设计

§ 5-1	中断与异常	(213)
5-1-1	8086/286 的中断方式	(214)
5-1-2	中断类型与中断向量	(216)
5-1-3	中断响应	(218)
5-1-4	中断返回	(219)
5-1-5	中断优先权	(221)
* 5-1-6	异常	(221)
5-1-7	可编程中断控制器 8259A	(222)
* 5-1-8	386 的中断与异常	(225)
§ 5-2	DOS 中断调用	(226)
5-2-1	DOS 操作系统	(226)
5-2-2	中断调用	(228)
5-2-3	中断调用的使用编程	(230)
§ 5-3	系统功能调用	(233)
5-3-1	系统功能调用	(233)
5-3-2	使用举例	(234)
5-3-3	常驻内存程序的设计	(238)
5-3-4	在程序中嵌套 DOS 命令行操作	(239)
§ 5-4	显示调用的程序设计	(244)
5-4-1	EGA 方式	(245)

5-4-2	VGA/TVGA 方式	(246)
5-4-3	10H 显示中断调用	(247)
* 5-4-4	VGA/TVGA 的直接 VRAM 访问	(261)
§ 5-5	磁盘文件管理	(270)
* 5-5-1	磁盘参数	(271)
* 5-5-2	磁盘分区	(271)
* 5-5-3	13H 磁盘中断调用	(275)
* 5-5-4	25H/26H 绝对磁盘读写中断调用	(277)
* 5-5-5	系统功能调用——传统的磁盘文件管理	(278)
5-5-6	采用文件标记的管理	(281)
§ 5-6	通信应用编程	(286)
5-6-1	信号处理	(287)
5-6-2	信号接收缓冲区与队	(289)
5-6-3	实时多任务与链表	(292)
5-6-4	信号编译码	(296)
习题五	(299)
实验题五	(300)

第六章 输入输出程序设计

§ 6-1	I/O 指令与并行通信	(302)
6-1-1	I/O 指令	(303)
6-1-2	以查询方式进行数据并行输入/输出	(304)
6-1-3	微机并行接口 (打印口)	(307)
6-1-4	打印机 I/O 中断调用 (17H)	(309)
* 6-1-5	打印控制命令	(310)
§ 6-2	串行通信与 8250 可编程异步通信接口	(312)
6-2-1	串行通信	(312)

6-2-2	RS 232C 接口标准	(313)
6-2-3	8250 可编程串行异步通信接口 (UART)	(315)
6-2-4	串行通信程序设计	(320)
6-2-5	串行输入输出中断调用与功能调用	(329)
§ 6-3	可编程定时/计数器 8253/8254 与音乐编程	(332)
* 6-3-1	8253 的编程	(333)
6-3-2	PC 微机扬声器驱动方法	(336)
6-3-3	音调控制	(337)
6-3-4	简单乐曲的演奏	(339)
习题六	(341)
实验题六	(341)

* 第七章 保护模式下的程序设计

§ 7-1	286 保护模式下的寻址实现	(344)
7-1-1	286 CPU 系统结构	(344)
7-1-2	寻址过程	(345)
7-1-3	段选择符与段描述符	(346)
7-1-4	门描述符	(351)
§ 7-2	地址管理与虚拟存储的实现	(353)
§ 7-3	特权级的保护	(354)
7-3-1	特权级 (Privilege Level)	(355)
7-3-2	堆栈与数据段特权级保护规则	(355)
7-3-3	代码段特权级保护规则	(356)
7-3-4	一致性代码段和非一致性代码段	(358)
7-3-5	代码段特权级检查细则	(360)
7-3-6	引起 CPL 变化的中断/异常与调用	(362)
7-3-7	其他保护性检查	(364)

7-3-8 I/O 保护	(364)
§ 7-4 286/386 的实地址模式	(365)
7-4-1 实地址模式	(365)
7-4-2 与 8086 的区别	(366)
7-4-3 由保护模式返回实模式的方法	(366)
§ 7-5 多任务与任务转换	(368)
7-5-1 多任务	(368)
7-5-2 任务状态段 TSS	(369)
7-5-3 任务门	(371)
7-5-4 任务转换	(371)
§ 7-6 保护模式下的中断与异常	(373)
7-6-1 实模式下的中断与异常	(373)
7-6-2 保护模式下的中断与异常	(373)
§ 7-7 保护模式下的指令扩充	(374)
§ 7-8 286 保护模式程序设计举例	(375)
7-8-1 一般性问题	(375)
7-8-2 程序实例	(379)
7-8-3 访问扩充内存	(388)
§ 7-9 386 保护模式程序设计	(390)
7-9-1 386 的保护模式	(390)
7-9-2 寻址 16 位段的设计举例	(392)
7-9-3 寻址 32 位段的设计举例	(393)
习题七	(398)
实验题七	(399)
参考文献	(400)
附录一 8086 汇编语言上机操作与常用工具软件	(402)
一. 上机操作过程	(402)

二. 汇编程序 MASM	(403)
三. 库程序 LIB	(404)
四. 连接程序 LINK	(404)
五. 动态调试程序 DEBUG	(405)
六. Code View 调试程序	(408)
附录二 DOS 系统功能调用表	(411)
附录三 8086/286 指令表	(418)
附录四 ASCII 字符表	(427)

绪 论

在计算机发展早期，人们用机器语言编制程序。随着计算机技术的发展，出现了汇编语言与各种高级语言。高级语言容易学习，通用性强，为各种行业的人们所熟知。但懂得汇编语言的，就往往局限于计算机、自控和通信电子领域的工作者。这是因为汇编语言与机型密切相关，掌握有一定难度。但是，汇编语言程序具有能与机器语言相媲美的时空效率，实时性强，因此又是以上领域的工作者，特别是计算机专业的学生所必须掌握的。目前，以 Intel 8086 系列微处理器为核心的微计算机，已获得广泛应用。因此，我们将以 Intel 8086 汇编语言为主，介绍汇编语言程序的一般设计方法，并适当兼顾介绍 80286/386。因为，从程序设计的角度看，8086 已包含了 286/386 的主要功能。

首先，我们回顾一下 20 年来微计算机发展的历史。70 年代以来，由于大规模集成电路的出现，微处理器和微型计算机从无到有，获得了空前的发展。当前，微计算机的应用已进入军事、航天、通信、仪表仪器、商业、医疗卫生、工业、农业乃至人们日常生活之中，为人们提供价廉、可靠、简便的智能化服务。我们今天对微型计算机如此依赖，以致于很难设想“离开微计算机，世界将会怎样”。微计算机对今后信息时代发展将产生的深远影响，这一点无论怎么估价也是不会过份的。

1971 年出现的 Intel 4004 4 位机，并不十分引人注目。真正使计算机世界重视的，是其后出现的 8 位机 8008，8080。以后，以 Intel 为例，陆续推出 8085A（1975 年），16 位机 8086（1976 年），8088（1977 年），80186，80286（1982 年），32 位机 80386（1985