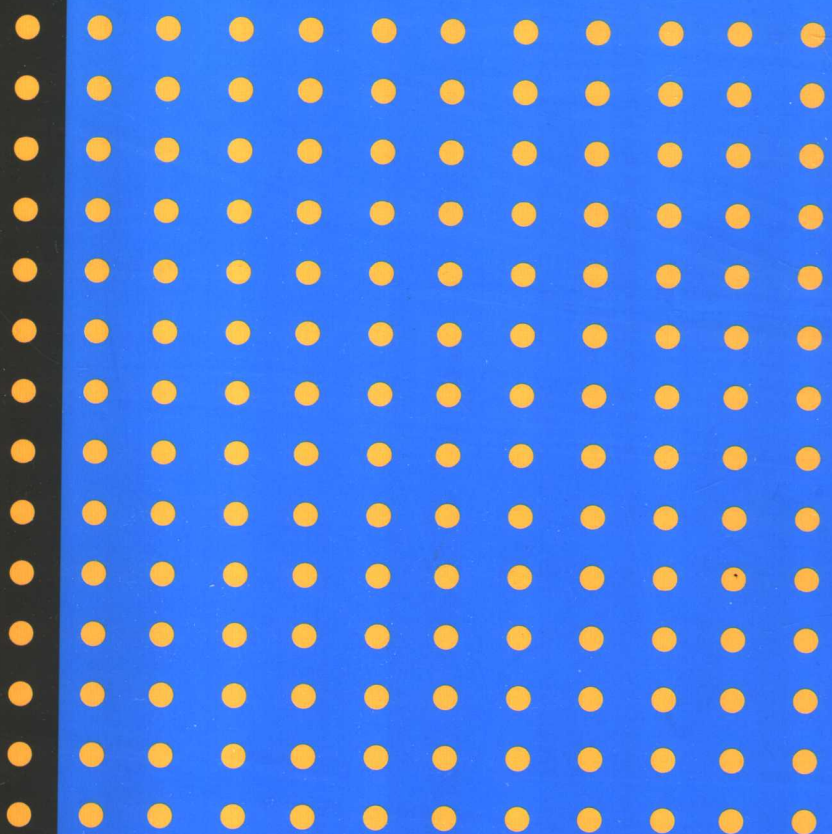
重点大学计算机专业系列教材

汇编语言程序设计
——从DOS到Windows

张雪兰　谭毓安　李元章　编著



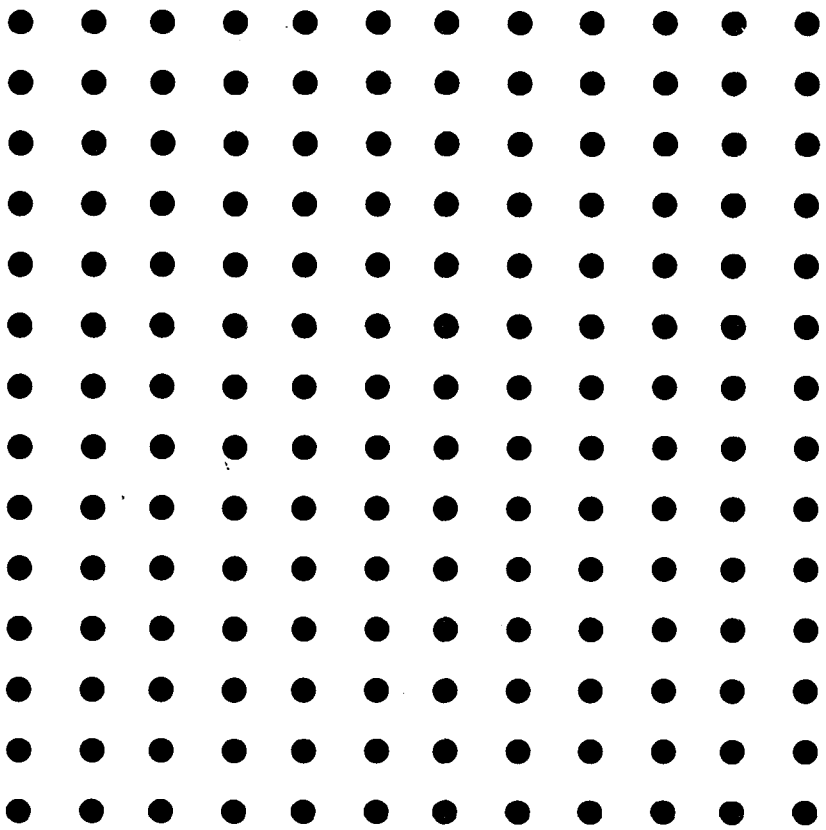
清华大学出版社

重点大学计算机专业系列教材

汇编语言程序设计

——从DOS到Windows

张雪兰　谭毓安　李元章　编著



清华大学出版社
北京

内 容 简 介

本书选择了当今广为流行的以 Intel 80x86 系列为 CPU 的 PC 及其兼容机作为硬件平台，以 DOS 和 Windows 两种操作系统作为软件平台，深入讨论实模式和保护模式的汇编语言程序设计。全书共分 12 章，由两部分组成。第 1 部分介绍 Intel 80x86 系列微处理器的基础知识、实模式汇编语言程序设计等，主要内容包括：预备知识、微处理器的基础知识、寻址方式及指令集、汇编语言程序组织、程序的基本结构及其程序设计、子程序与宏指令设计、实模式 I/O 程序设计、汇编语言高级编程技巧等。第 2 部分介绍基于 Windows 的保护模式程序设计，主要内容包括：32 位 CPU 及 Windows 基础、Windows 汇编语言程序设计基础、深入 Windows 汇编编程、保护模式及其应用等。本书内容由浅入深、循序渐进、实例丰富，许多完整程序都是有一定难度的实际应用，很有参考价值。本书每章后均附有习题，以便读者检查及巩固所学知识。

本书既可作为高等院校计算机科学与技术专业及其相关专业的本科教材，也可供从事计算机开发及研究的工程技术人员参考。

图书在版编目(CIP)数据

汇编语言程序设计：从 DOS 到 Windows/张雪兰，谭毓安，李元章编著．—北京：清华大学出版社，2006.4
（重点大学计算机专业系列教材）
ISBN 7-302-12436-1

Ⅰ.汇…　Ⅱ.①张…　②谭…　③李…　Ⅲ.汇编语言－程序设计－高等学校－教材　Ⅳ.TP313

中国版本图书馆 CIP 数据核字(2006)第 005682 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：索　梅
文稿编辑：李玮琪
印 刷 者：北京市清华园胶印厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：29.75　**字数**：702 千字
版　　次：2006 年 4 月第 1 版　2006 年 4 月第1 次印刷
书　　号：ISBN 7-302-12436-1/TP・7975
印　　数：1～4000
定　　价：38.00 元

INTRODUCTION

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科，它们多数都集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

2. 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系

时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系，基本教材与辅助教材以及教学参考书的关系，文字教材与软件教材的关系，实现教材系列资源配套。

5. 依靠专家，择优落实。在制定教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

FOREWORD

前言

汇编语言是一种程序设计语言，是当今时空性最好、直接控制硬件底层能力最强的语言。通过它可以对计算机系统中所发生的事件进行精确控制，把系统的功能发挥到淋漓尽致。汇编语言是一种符号化了的机器语言，与硬件系统密切相关，面对目前 CPU 越来越强大、越来越复杂的功能，使用汇编语言编写高性能的程序极具挑战性。

汇编语言程序设计是高等院校计算机科学与技术专业本科生的一门必修课。它不仅能够训练学生编写高效率、直接控制硬件的汇编源程序及掌握程序设计技术，而且对于学生了解计算机内部运行机制、加深对相关课程的理解、运用调试工具准确分析程序错误、剖析可执行程序(因商业机密等原因无法获得源程序)的关键代码、程序优化等都有着很重要的作用。

由于汇编语言本身的特点，学习汇编语言离不开实际的计算机系统，因此，选择一个典型的系统，不仅对于组织教材是重要的，而且对于理论联系实际地进行教学也是十分必要的。本教材选择了当今广为流行的以 Intel 80x86 系列为 CPU 的 PC 及其兼容机作为硬件平台，深入讨论汇编语言程序设计。众所周知，Intel CPU 经历了从 16 位的 8086 到 32 位的 80386～Pentium，直到 64 位的 Itanium。在体系结构发展、指令集与寄存器扩充的同时，运行模式也从实模式发展到保护模式。为了体现时代性，本教材介绍两种工作模式的编程，并把内容组织成两部分。第 1 部分介绍 Intel 80x86 系列微处理器的基础知识、实模式汇编语言程序设计等，它不仅可以满足目前大部分控制硬件的编程需要及程序短小紧凑的要求，还是学习保护模式编程的基础。另外，由于 Intel CPU 系列良好的向下兼容性，绝大多数的实模式程序可以不加改变而直接运行在虚拟 8086 模式下。因此，到目前为止，实模式编程仍然有广泛的应用领域。第 2 部分介绍了基于 Windows 的保护模式程序设计及其技术基础，保护模式程序突破了实模式只能访问常规内存等许多局限，可以充分发挥 80386 及其以上 CPU 的强大功能。全书

共分 12 章，内容包括：预备知识、微处理器的基础知识、实模式的寻址方式及指令集、汇编语言程序组织、程序基本结构及其程序设计、子程序与宏指令设计、实模式 I/O 程序设计、汇编语言高级编程技巧、32 位 CPU 及 Windows 基础、Windows 汇编语言程序设计基础、深入 Windows 汇编编程、保护模式及其应用等，并在附录中给出了汇编语言伪指令和操作符、DEBUG 调试工具、DOS 系统功能调用、BIOS 中断调用、DEBUG 调试工具的参考资料，以方便读者查阅。书中提供了大量具有一定难度的程序实例，很有参考价值。这些例子均能在采用 Intel P4 和 AMD 等兼容 CPU 的微型计算机上正确运行。另外，本书每章后均附有习题，便于读者检查及巩固所学知识。

本书的第 2 章、第 4 章～第 8 章由张雪兰教授编写，第 9 章～第 12 章由谭毓安副教授编写，第 1 章、第 3 章及附录由李元章编写，全书由张雪兰统稿。在编写过程中，作者不仅融汇了多年主讲本课程的教学经验和科研积累，还得到了许多同志的热情帮助和建议，在此深表谢意，并对所参考的国内外教材和资料的原作者表示衷心的感谢。

对书中的错误和不妥之处，敬请读者批评指正。

本书配有配套的电子课件，读者可到清华大学出版社网站(www. tup. tsinghua. edu. cn)上免费下载。

编者

2006 年 2 月

CONTENTS

目录

第1部分　实模式编程

第2部分 保护模式编程

第1部分　实模式编程

Intel CPU 经历了从 16 位的 8086 到 32 位的 80386～Pentium，直到 64 位的 Itanium。在体系结构发展、指令集与寄存器扩充的同时，工作模式也从实模式发展到保护模式。实模式是上述 CPU 均支持的一种工作模式，每次机器冷启动或复位都隐含地以实模式开始工作。实模式也是 DOS 操作系统所依赖的工作模式，DOS 自身、BIOS、I/O 服务程序、设备驱动程序、TSR 程序、DOS 应用程序等都被设计成在实模式下工作。实模式下的编程技术成熟，程序短小紧凑，运行速度快，有很高的灵活性，它不仅可以满足目前大部分控制硬件的编程需要，而且还是学习保护模式编程的基础。另外，由于 Intel CPU 系列良好的向下兼容性，绝大多数的实模式程序可以不加改变而直接运行在虚拟 8086 模式下。因此到目前为止，实模式编程仍然有着广泛的应用领域。本部分包括预备知识、Intel 80x86 系列微处理器基础知识、实模式汇编语言程序设计等，这些基础知识、实模式编程思想及技巧对保护模式程序设计同样适用。

CHAPTER 1

预备知识　第1章

1.1 进位记数制及不同数制间的转换

1.1.1 什么是进位记数制

进位记数制是指用一组固定的数字符号和统一的规则表示数的方法。讨论进位记数制要涉及到两个基本问题：基数和权。在进位记数制中，一种计数制允许选用基本数字符号的个数叫做基数。例如人们习惯使用的十进制，是采用0～9这10个数字表示的，它的基数是10。在一个数中，数字在不同的数位所代表的值是不同的，每个数字所表示的数值等于它本身乘以与所在数位有关的常数，把这个常数叫做位权，简称权。例如十进制数个位的位权是1，十位的位权是10，百位的位权是100，千位的位权是1000……。相邻两位权的比值就等于基数。一个数的数值大小就等于它的各位数码乘以相应位权的总和。例如：

十进制数 $2698=2\times1000+6\times100+9\times10+8\times1$

在日常生活中，人们经常使用十进制、十二进制、六十进制等。

1.1.2 计算机中常用的进位记数制

在计算机中，常使用的有二进制、八进制、十进制、十六进制，具体见表1-1。

1. 十进制

十进制数的特点是用10个数码(0～9)表示所有的数，10为基数，计数方法是逢10进1。例如十进制数3678.5可以表示为：

$3678.5=3\times10^3+6\times10^2+7\times10^1+8\times10^0+5\times10^{-1}$