普通高校本科计算机专业特色教材精选·算法与程序设计

汇编语言基础及驱动程序开发

戴水贵 等 编著

清华大学出版社

普通高校本科计算机专业特色教材精选·算法与程序设计

汇编语言基础及驱动程序开发

戴水贵 敖志刚 俞海英 冯小明 编著

清华大学出版社
北京

内 容 简 介

本书对汇编语言作了全面介绍，并通过程序实例详细讲解了用汇编语言开发驱动程序的方法。全书共7章。第1章～4章为汇编语言基础知识，第5章～7章是用汇编语言开发驱动程序。本书适用于汇编语言初学者，同时又是用汇编语言开发驱动程序的入门书。

驱动程序涉及的内容比较多，本书以程序例的形式给出程序，让读者有整体概念，并在程序例中给出比较多的注释，使读者读完一个程序后知道如何解决此类问题，并起到举一反三的作用。

图书在版编目（CIP）数据

汇编语言基础及驱动程序开发 / 戴水贵等编著. —北京：清华大学出版社，2012.3
（普通高校本科计算机专业特色教材精选·算法与程序设计）
ISBN 978-7-302-26649-5

Ⅰ. ①汇… Ⅱ. ①戴… Ⅲ. ①汇编语言－驱动程序－程序设计－高等学校－教材 Ⅳ. ①TP313

中国版本图书馆CIP数据核字(2011)第179125号

责任编辑：袁勤勇　战晓雷
封面设计：常雪影
责任校对：李建庄
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：20.75　　**字　数**：521千字
版　　次：2012年3月第1版　　**印　次**：2012年3月第1次印刷
印　　数：1～3000
定　　价：29.00元

产品编号：042718-01

出版说明

INTRODUCTION

在我国高等教育逐步实现大众化后，越来越多的高等学校将会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为此，教育部已经启动了“高等学校教学质量和教学改革工程”，强调要以信息技术为手段，深化教学改革和人才培养模式改革。如何根据社会的实际需要，根据各行各业的具体人才需求，培养具有特色显著的人才，是我们共同面临的重大问题。具体地说，培养具有一定专业特色的和特定能力强的计算机专业应用型人才则是计算机教育要解决的问题。

为了适应21世纪人才培养的需要，培养具有特色的计算机人才，急需一批适合各种人才培养特点的计算机专业教材。目前，一些高校在计算机专业教学和教材改革方面已经做了大量工作，许多教师在计算机专业教学和科研方面已经积累了许多宝贵经验。将他们的教研成果转化为教材的形式，向全国其他学校推广，对于深化我国高等学校的教学改革是一件十分有意义的事情。

清华大学出版社在经过大量调查研究的基础上，决定组织出版一套“普通高校本科计算机专业特色教材精选”。本套教材是针对当前高等教育改革的新形势，以社会对人才的需求为导向，主要以培养计算机应用型人才为目标，立足课程改革和教材创新，广泛吸纳全国各地的高等院校计算机优秀教师参与编写，从中精选出版确实反映计算机专业教学方向的特色教材，供普通高等院校计算机专业学生使用。

本套教材具有以下特点：

1. 编写目的明确

本套教材是在深入研究各地各学校办学特色的基础上，面向普通高校的计算机专业学生编写的。学生通过本套教材，主要学习计算机科学与技术专业的基本理论和基本知识，接受利用计算机解决实际问题的基本训练，培养研究和开发计算机系统，特别是应用系统的基本能力。

2. 理论知识与实践训练相结合

根据计算学科的三个学科形态及其关系，本套教材力求突出学科的理论与实践紧密结合的特征，结合实例讲解理论，使理论来源于实践，又进一步指导实践。学生通过实践深化对理论的理解，更重要的是使学生学会理论方法的实际运用。在编写教材时突出实用性，并做到通俗易懂，易教易学，使学生不仅知其然，知其所以然，还要会其如何然。

3. 注意培养学生的动手能力

每种教材都增加了能力训练部分的内容，学生通过学习和练习，能比较熟练地应用计算机知识解决实际问题。既注重培养学生分析问题的能力，也注重培养学生解决问题的能力，以适应新经济时代对人才的需要，满足就业要求。

4. 注重教材的立体化配套

大多数教材都将陆续配套教师用课件、习题及其解答提示，学生上机实验指导等辅助教学资源，有些教材还提供能用于网上下载的文件，以方便教学。

由于各地区各学校的培养目标、教学要求和办学特色均有所不同，所以对特色教学的理解也不尽一致，我们恳切希望大家在使用教材的过程中，及时地给我们提出批评和改进意见，以便我们做好教材的修订改版工作，使其日趋完善。

我们相信经过大家的共同努力，这套教材一定能成为特色鲜明、质量上乘的优秀教材。同时，我们也希望通过本套教材的编写出版，为“高等学校教学质量和教学改革工程”做出贡献。

清华大学出版社

前言

PREFACE

提起汇编语言，人们的第一感觉就是难学、编程麻烦。但我要告诉你，在Windows操作系统下，汇编语言已不再难学，汇编语言已同样具有高级语言的特点。例如，汇编语言也有.if~else，.while，.forc等语句，更为难能可贵的是：汇编语言更加直接地面对操作系统，而且没有高级语言那么多条条框框和人为的再封装，使读者更加容易掌握。汇编语言的编译和连接环境更加简单方便。

在用汇编语言编写驱动程序之前，我也曾试图用C语言来写这部分内容，但再三比较之后，我最后还是选用汇编语言。原因是：C语言总是有“云里雾里”的感觉，只能硬记其用法，很难理解其中的含义。造成这种感觉的原因是C语言的再封装造成的。

在C语言中，驱动程序的编译、连接显得比较麻烦，而在汇编语言中显得很方便（将汇编语言程序写成.bat形式，再将编译、连接命令放在源程序中，只要运行.bat程序，就可生成.sys文件）。

在Windows汇编语言程序设计中，真正用汇编语言指令写程序的机会并不多，原因是可以调用系统提供的API函数解决问题。在汇编语言中定义过程、结构体、共用体等也十分方便。汇编语言中的知识库（后缀为.inc的头文件）可以用相应的工具软件将C语言中的头文件（后缀为.h）转换而得，因而，汇编语言同样有强大的后备知识库资源。

学习汇编语言的另一个好处是：不管可执行程序是用何种语言编写的，用反汇编工具（如IDA）反汇编出的程序都是汇编语言程序（以API函数的形式给出），稍加修改后，可将反汇编出的程序再编译、连接成可执行程序。可见，掌握了汇编语言后，能学到书本上没有的东西。

在编写驱动程序之前，我反复想过如何写这部分内容的问题。因为驱动程序很复杂，涉及的知识面很广。如果将每个必要的知识点都一一列出，并加以说明，则显得支离破碎，像流水账或手册，且要占用很大的篇幅。这种讲法只能把知识堆积在书中（甚至可能会成为手册），使读者没有整体概念，且不会用，效果肯定不好。针对以上原因，我决定用

小的程序实例的方法来写这部分内容。抓住重点，把整体框架交给读者，让读者通过小的程序实例掌握其中的含义和用法。但是，这种讲解方法也有缺点。例如，一上来就用小的程序实例来讲解，加之再小的程序实例也不会小，使读者一开始就会遇到很多没有见到过的内容，一下子可能会被吓倒！希望读者一定要渡过这个难关，带着问题到开发环境的有关头文件（如 ntddk.inc 等）中慢慢领会。当然，我尽量结合程序实例多做一些讲解，并在程序中多给出一些注释。

一般的书都喜欢在给出完整程序后（程序中的注释比较少），再在程序后给出大量的讲解，我觉得这种方法不好（我喜欢在程序中加注释，这样读起来更直接）。

驱动程序的安装与运行方法比较特殊，如果驱动程序有错误，安装、运行后将会导致死机（出现蓝屏），并使计算机无法再启动，因而要特别注意。

本书可作为高等院校的教材，也适合作为自学者的入门读物。

戴水贵

2011 年 12 月

目录

CONTENTS

第1章 Windows汇编语言基础知识

CHAPTER

1.1 如何学习Windows汇编语言

汇编语言是在机器语言之上的助记符语言，即用符号来表示二进制码，以便用户记忆。例如，指令MOV AX,1234是将数1234送到AX寄存器，这条指令编译后是一个二进制数。本书不详细讲解指令及一些基本算法，否则就又回到DOS汇编语言了。本书把指令系统详细列出，并给出简短的程序实例，使读者更容易学会指令的使用方法。

由于编译系统提供了很多高级语法，使Windows汇编语言与高级语言已很相似，因此，在注意掌握基本指令的基础上，应把注意力放在如何用汇编语言指令或伪指令调用Windows提供的API函数上。这样才能体现出Windows汇编语言的特点。

1.2 Windows汇编语言与DOS汇编语言的区别

在DOS和Windows操作系统下，80x86芯片的指令系统是一样的。在DOS操作系统实模式下，寄存器都是16位的，要访问1MB的内存空间，必须用分段的概念(因为$2^{16}=10000h=64KB$，即寻址范围是0000～0FFFFh，只能访问64KB，详细原理见本书第4章4.1节)，因而提出了相对地址的概念。这个概念给学DOS汇编的人带来了很大难度。

在Windows操作系统下，寄存器都是32位的($2^{32}=100000000h=4GB$，寻址范围是00000000～0FFFFFFFFh，即能访问4GB)。这使Windows汇编语言可以工作在平坦模式，即没有分段的概念，因此也使Windows汇编语言比DOS汇编语言更好学(再也没有分段的麻烦了)。

在DOS操作系统下，用户可以用汇编语言指令访问计算机的所有资源。而在Windows操作系统下，汇编语言中的一些特权指令(如IN、OUT等)是不许用户使用的，除非用户编写了驱动程序。微软这样做是为了操作系统自身的安全，但也给用户开发程序带来了不便。

在DOS操作系统下，用户可以用系统BIOS提供的调用口 int 13h 直接访问硬盘，而在Windows操作系统下是不能使用 int 13h 的。要直接访问硬盘，必须使用Windows操作系统提供的API调用函数。

1.3 二进制数

1.3.1 将十进制数转为二进制、八进制和十六进制数

关于将十进制数转为二进制数的方法，一般的书中都给出“除2求余”的方法，这种方法用起来不方便。下面给出一种计算比较快的方法。

1. 将十进制整数转为二进制数

任何一个整数都是由以下数中的一些数相加的结果：

$2^0=1$	$2^5=32$	$2^{10}=1024$	$2^{15}=32768$
$2^1=2$	$2^6=64$	$2^{11}=2028$	$2^{16}=65536$
$2^2=4$	$2^7=128$	$2^{12}=4096$	$2^{17}=131072$
$2^3=8$	$2^8=256$	$2^{13}=8192$	$2^{18}=262144$
$2^4=16$	$2^9=512$	$2^{14}=16384$	$2^{19}=524288$

例 1-1 将十进制数31转为二进制数。

```
  31
 -16  ──→ 2^4
 ---
  15
  -8  ──→ 2^3
 ---
   7                31=2^4+2^3+2^2+2^1+2^0
  -4  ──→ 2^2       即
 ---
   3                31(十进制)= 1 1111(二进制)
  -2  ──→ 2^1
 ---
   1
  -1  ──→ 2^0
 ---
   0
```

例 1-2 将8193转为二进制数。

```
 8193
-8192  ──→ 2^13
-----
    1
   -1  ──→ 2^0
-----
    0
```

8193(十进制)=10 0000 0000 0001(二进制)

2. 将十进制小数转为二进制数

任何一个小数都是由以下数中的一些数相加的结果：

$$2^{-1}=0.5$$
$$2^{-2}=0.25$$
$$2^{-3}=0.125$$
$$2^{-4}=0.0625$$

例 1-3　将十进制数 0.625 转为二进制数。

$$\begin{array}{r} 0.625 \\ -0.5 \quad \longrightarrow 2^{-1} \\ \hline 0.125 \\ -0.125 \quad \longrightarrow 2^{-3} \\ \hline 0 \end{array}$$

0.625(十进制数)=.101(二进制数)

注意：小数有除不尽(除 2)的数，对于小数点后的数，只要达到一定的精度后，其余的数就可舍弃。如果一个数既有整数部分，又有小数部分，则分别转换，转换后加入小数点就可以了。

3. 将十进制数转为八进制数和十六进制数

将十进制数转为二进制数后，再转为八进制数和十六进制数就很简单了。规则如下。

1) 整数

将二进制整数从右往左 3 位一组(不够时左边补 0)进行转换，便成为八进制数。

将二进制整数从右往左 4 位一组(不够时左边补 0)进行转换，便成十六进制数。

2) 小数

将二进制小数从左往右 3 位一组(不够时右边补 0)进行转换，便成为八进制数。

将二进制小数从左往右 4 位一组(不够时右边补 0)进行转换，便成为十六进制数。

例如，十进制数 0～32 对应的二进制、八进制和十六进制数如下：

十进制(d)	二进制(b)	八进制(o)	十六进制(h)
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D

14	1110	16	E
15	1111	17	F
16	10000	20	10
17	10001	21	11
18	10010	22	12
19	10011	23	13
20	10100	24	14
21	10101	25	15
22	10110	26	16
23	10111	27	17
24	11000	30	18
25	11001	31	19
26	11010	32	1A
27	11011	33	1B
28	11100	34	1C
29	11101	35	1D
30	11110	36	1E
31	11111	37	1F
32	100000	40	20

注意：

(1) 二进制数有 2 个状态：0、1(逢 2 进 1)。

(2) 八进制有 8 个状态：0、1、2、3、4、5、6、7(逢 8 进 1)。

(3) 十六进制有 16 个状态：1、2、3、4、5、6、7、8、9、A、B、C、D、E、F(10 为 A，11 为 B，…)。

1.3.2 计算机内存中的数是以二进制表示的

计算机硬件中单稳态电路的两个状态(高/低)正好对应 1 和 0。计算机内存中的数是以二进制表示的，任何一个数都是由 0 和 1 组成的。在用汇编语言写程序时，可以用十进制数(D)、八进制数(O 或 Q)、十六进制数(H)或二进制数(B)表示一个数，例如：

```
MOV AL,13D                ;将十进制数 13 送入 AL 寄存器(字符 D 可省略)
MOV AL,15O                ;将八进制数 15 送入 AL 寄存器
MOV AL,0DH                ;将十六进制数 0D 送入 AL 寄存器
MOV AL,00001101B          ;将二进制数 00001101 送入 AL 寄存器
```

在上述语句中，字母 D、O(或 Q)、H 及 B 也可以小写。

以上 4 条语句经过编译连接后，当用调试工具查看时的显示结果如下：

```
MOV AL,0D                 ;0D 为二进制数的十六进制显示
```