PC-DOS

操作系统详解

张桂平 贾厚光

北京联想计算机集团公司
一九九〇年八月

PC-DOS 操作系统详解

张桂平　贾厚光　编著

北京联想计算机集团公司

内 容 简 介

本书对 PC-DOS 的标准版本进行了详细解剖。全面系统地介绍了 PC-DOS 的构造、PC-DOS 的引导过程、磁盘引导装入程序、基本输入输出系统（IBMBIO.COM）、DOS 核心（IBMDOS.COM）、命令解释器（COMMAND.COM）的功能。全书彻底揭开了 PC-DOS 的全部奥秘。

本书可作为大专院校计算机专业的教学用书，或各企事业单位技术人员的培训教材及参考书。

前　言

随着 IBM-PC 及其兼容机的广泛普及，DOS 操作系统已成为一种最流行的单用户操作系统。用户和软件设计人员天天在和 DOS 操作系统打交道，然而很少有人知道它的内部结构，在编程实践中，常常因此而一筹莫展。为了帮助用户解决这个困难，我们对 PC-DOS 的标准版本进行了解剖，经过整理，编著了《PC-DOS 操作系统详解》，以下简称《详解》。

《详解》，作为我国的第一本真正详细解剖 PC-DOS 操作系统的专著，具有以下特点：

1. 以源代码形式给出了 IBMBIO.COM、IBMDOS.COM、COMMAND.COM 的源程序清单，对其中的每一条指令及各功能模块作了详细解释，可以不加修改经汇编、连接，产生可正确运行的目标代码。这样，人们可以随心所欲地对 PC-DOS 加以修改，扩展 PC-DOS 的功能，产生满足自己特定需要的全新的操作系统。

2. 首次公布了 PC-DOS 操作系统的全部资源，彻底揭开了 PC-DOS 的全部奥秘，打破了长期以来人们对 PC-DOS 的神秘感。人们可以利用 PC-DOS 的一些内部功能，更加有效地编写系统程序和应用程序（如网络通信程序、软件加密和解密程序等等）以及进行硬件测试和故障分析。

《详解》共有五章和一个附录。第一章详细介绍了 PC-DOS 的构造和 PC-DOS 的引导过程。第二章至第五章分别详细介绍了磁盘引导装入程序、基本输入输出系统（IBMBIO.COM）、DOS 核心（IBMDOS.COM）、命令解释器（COMMAND.COM）的功能、所采用的重要数据结构以及源程序的详细注释。附录中列出了 DOS 各个中断的功能，以便读者查阅。

《详解》涉及面广泛，内容丰富，便于读者阅读和掌握高深的操作系统知识，既可作为各大专院校计算机专业的教学用书，或各企事业单位技术人员的培训教材，也可作为广大从事微机科研、生产、应用开发的科技人员的参考书。

参加《详解》编写工作的人员有：张桂平（编写第三章、第四章和第五章）、贾厚光（编写第一章、第二章和附录）。

对 PC-DOS 进行解剖，且将目标代码符号化，是一项艰巨而又细致的工作，共花费了 4 年的心血。尽管笔者作出了种种努力，但其错误仍然在所难免，望广大读者提出修改意见。

作者

1990 年

[作者简介] 张桂平，男，1963年出生。1983年7月毕业于中南工业大学计算机系。1983年9月至1985年5月在天津市工业自动化仪表研究所从事单回路控制器的设计，1985年5月至1989年4月在湖南省涟源钢铁厂计算机站从事MIS系统的软件开发，1989年4月至今，在长沙前进计算机研究所进行系统软件的开发。

张桂平与计算机系统软件结下了不解之缘。他涉及了计算机系统软件的大多数领域，在系统软件方面作了大量工作。其主要工作有：

1. 研究软件加密和解密技术；
2. 阅读dBASEⅢ PLUS的系统程序，编写了反编译程序UNDBC；
3. 阅读PLAN 5000网络系统程序，编写了实时电子邮政程序，在国际计算机通信会议（ICCC SYMPOSIUM '89）上发表了有关论文；
4. 设计工具软件（反汇编软件、表格编辑器、图形软件包、排版软件等）；
5. 系统软件的汉化；
6. 详细解剖PC-DOS操作系统。

目　录

第一章　PC-DOS 的构造及其加载过程

PC-DOS 操作系统分为几层，以便于将其运行的硬件与 PC-DOS 的核心逻辑隔离开，这样对用户而言，硬件是透明的。这些层次是:

(1) 基本输入输出系统（IBMBIO.COM）

(2) DOS 核心（IBMDOS.COM）

(3) 命令解释器（COMMAND.COM）

PC-DOS 各层次的功能特点见下表。

名　称	功　能　特　点
IBMBIO.COM	依赖机器硬件，扩充了 ROM BIOS 与 IBMDOS.COM 接口，处理同全体外设的通讯。
IBMDOS.COM	不依赖机器硬件，与 IBMBIO.COM、COMMAND.COM 和应用程序接口。初始并控制与全体外设的通讯；处理终端、打印机、键盘的输入、输出，含有完整的 PC-DOS 文件系统。
COMMAND.COM	常驻部分：处理程序退出、Ctrl-Break 键、致命错误中断，与 IBMDOS.COM、用户程序、COMMAND.COM 的暂驻内存部分接口；程序结束时检查暂驻部分的完整性，不完整的话则重新装入；报告致命错误。暂驻部分：与 COMMAND.COM 的常驻部分、IBMDOS.COM 和操作员接口；含有 COPY、DEL、TYPE、RENAME 等内部命令处理程序；控制批处理文件，进行批处理；加载程序并执行。

DOS 的加载过程如下:

1. 当系统加电或热启动后，程序从 0FFFF0H 开始执行，进入自检程序和 ROM 引导装入程序（见图 1-1）。

2. ROM 引导装入程序，从磁盘的第 1 扇区（引导扇区）读入磁盘引导装入程序到 0:7C00H，然后将控制权转交给磁盘引导装入程序（见图 1-2）。

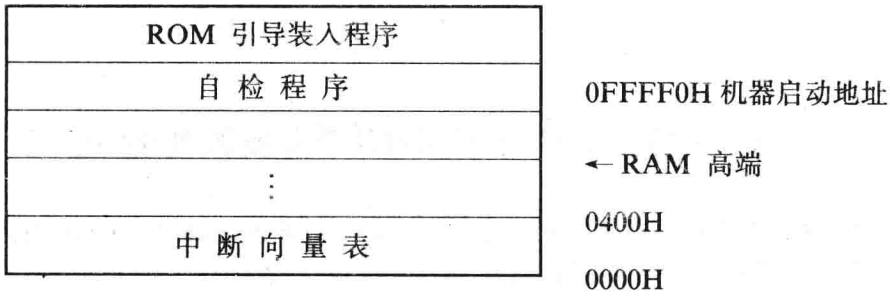

图 1-1

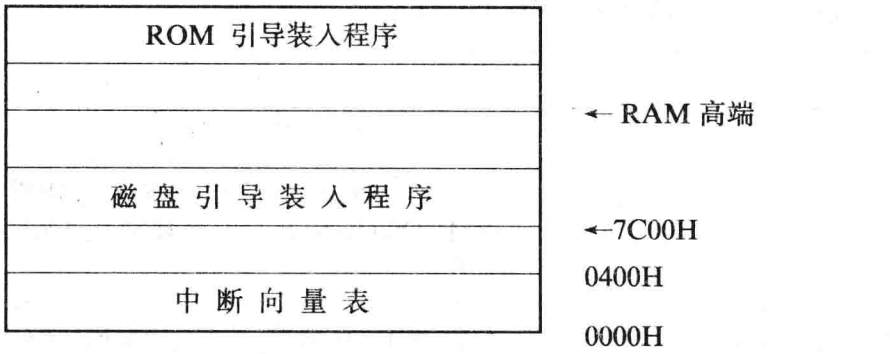

图 1-2

3. 磁盘引导装入程序检查盘上有无 DOS 系统。检查过程为：读入根目录的第 1 扇区，然后检查其中前两个文件是否为 IBMBIO.COM 和 IBMDOS.COM，若盘上无这两个文件，系统将提示用户插入另一磁盘，然后按下任一键继续。若发现了这两个文件，磁盘引导装入程序便将 IBMBIO.COM 读入内存，并将控制转向 IBMBIO.COM 的初始化入口（见图 1-3）。

4. IBMBIO.COM 由两模块组成：第 1 个模块是 BIOS，它由一组设备驱动程序组成；第 2 个模块是 SYSINIT。

BIOS 模块的初始化部分将 IBMDOS.COM 加载到内存（见图 1-4）。

5. SYSINIT 由 BIOS 的初始化代码调用。该程序确定连续的内存空间的大小，然后将自身重新装入内存高端。然后，SYSINIT 将 DOS 核心（IBMDOS.COM）从初始位置重新加载到最后位置，并将 IBMBIO.COM 中可覆盖的初始化程序和内存低端的 SYSINIT 覆盖掉（见图 1-5）。

6. 随后，SYSINIT 调用 IBMDOS.COM 的初始化程序。作为系统初始化工作的一部分，DOS 核心检查由驻留的块设备驱动程序返回的磁盘参量，确定系统所使用最大的扇区的大小，建立一些磁盘参数块（DPB），并设立磁盘缓冲区。

执行完 DOS 核心的初始化程序后，SYSINIT 便可调用 DOS 的文件服务程序（INT 21H）去打开 CONFIG.SYS 文件，用户可在 CONFIG.SYS 中指定新加的设备驱动程序，确定磁盘缓冲区的数目，最多可同时打开的文件数目以及定义命令解释器的文件名等（见图 1-6）。

7. 加载完所有可安装的设备驱动程序后，SYSINIT 关闭所有的文件指针，重新打开控制台（CON）、打印机（PRN）以及辅助设备（AUX）。此时允许用户安装的字符设备驱动程序覆盖掉 BIOS 为标准设备驻留的设备驱动程序。

最后，SYSINIT 调用 DOS 的 EXEC 功能将命令解释器（COMMAND.COM）加载到内存，然后将控制转交给命令解释器。

命令解释器显示 DOS 提示符，等待用户输入命令。此时 DOS 进入正常工作状态，SYSINIT 消失（见图 1-7）。

图 1-3

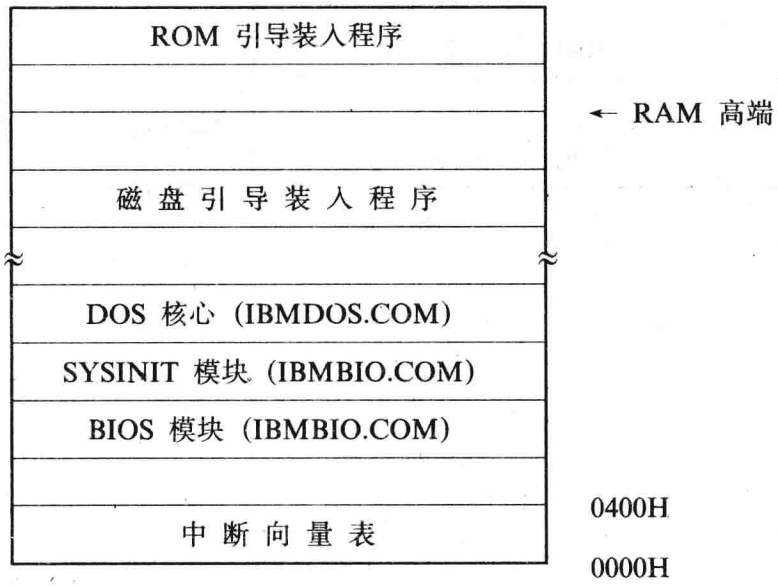

图 1-4

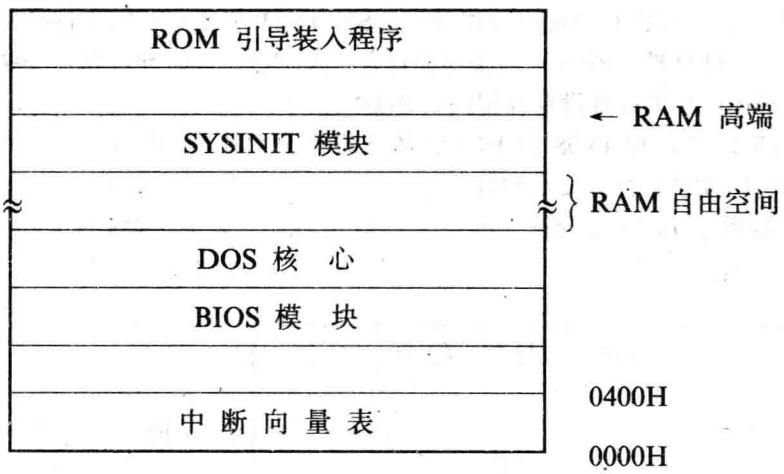
ROM 引导装入程序
SYSINIT 模块
← RAM 高端
RAM 自由空间
DOS 核 心
BIOS 模 块
中 断 向 量 表
0400H
0000H

图 1-5

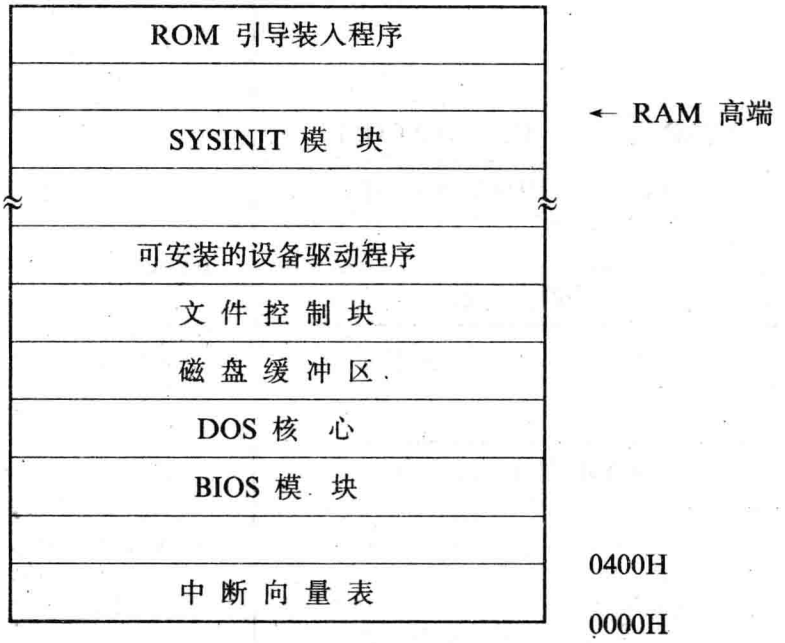
ROM 引导装入程序
SYSINIT 模 块
← RAM 高端
可安装的设备驱动程序
文 件 控 制 块
磁 盘 缓 冲 区
DOS 核 心
BIOS 模 块
中 断 向 量 表
0400H
0000H

图 1-6

图 1-7

第二章　磁盘引导装入程序

磁盘引导装入程序处于磁盘的第 1 扇区（引导扇区），它的结构如下图所示：

EB XX 90 (JMP LABEL)
OEM 名和版本
BIOS 参数块 (BPB)
磁 盘 参 数 表
引 导 程 序 55 AA

磁盘引导装入程序检查磁盘目录中的第 1 块里面是否有 IBMBIO.COM 文件和 IBMDOS.COM 文件，若找到了这两个文件，则认为该盘是可以引导的，于是将文件区开始连续的扇区（即 IBMBIO.COM 文件）读入内存（开始地址为 0070H:0），然后执行之。若没有找到这两个文件，引导程序显示“Non-System disk or disk error”，然后等待用户按下任一键后，跳转到 ROM 引导装入程序再次引导。

磁盘引导装入程序的清单如下：

```
;       BOOT.ASM — 磁盘引导程序(软盘)
;       按如下步骤形成执行代码:
;           C> MASM BOOT;
;           C> LINK BOOT;
;           C> DEBUG BOOT.EXE
;             -N BOOT.DAT
;             -RCX
;             :200
;             -WCS:7C00
;             -Q
Lf          EQU     10                  ; 换行符
Cr          EQU     13                  ; 回车符
CodeSeg     SEGMENT PARA PUBLIC 'CODE'
            ASSUME  CS:CodeSeg
            ORG     7C00H
```

```
Start:    JMP     Main
Dir_Area  LABEL   WORD                    ; 存放根目录的起始扇区号
TempUnit  EQU     THIS WORD+5
          DB      "IBM  2.0"              ; OEM 标志
Byte1Sect DW      200H                    ; 每扇区字节数          ┐
          DB      2                       ; 每簇扇区数            |
Resv_Sect DW      1                       ; 保留扇区数            |
FATs      DB      2                       ; FAT数目               |
Directory DW      112                     ; 根目录中的目录项数    |
Sectors   DW      02D0H                   ; 扇区总数              | BIOS参数
SectorNo  LABEL   BYTE                    ; 存放扇区号            | 块(BPB)
Media     DB      0FDH                    ; 介质描述字节          |
S_1FAT    DW      2                       ; 单个FAT的扇区数       |
S_1Track  DW      9                       ; 每磁道扇区数          |
DiskSide  DW      2                       ; 磁头数                |
S_1Part   DW      0                       ; 第1分区的相对扇区号   ┘
DrvNo     DB      0                       ; 驱动器号
Head      DB      0                       ; 磁头号
BIO_Len   DB      10                      ; IBMBIO.COM 的长度(以簇为单位)
DPT       DB      0DFH                    ; 磁盘参数表
          DB      2
          DB      25H
          DB      2
          DB      9
          DB      2AH
          DB      0FFH
          DB      50H
          DB      0F6H
          DB      0
          DB      2
;
Main      PROC    FAR
          CLI                             ; 禁止中断
          XOR     AX,AX                   ;┐
          MOV     SS,AX                   ;| 设置堆栈
          MOV     SP,OFFSET Start         ;┘
          MOV     DS,AX                           ;┐
          MOV     DS:[007AH],AX                   ;| 设置磁盘参数表
          MOV     WORD PTR DS:[0078H],OFFSET DPT  ;┘
```

```
        STI                             ; 开放中断
        INT     13H                     ; 重启动磁盘
        JNC     Main_1                  ; 正确
        JMP     Main_7                  ; 出错: "Disk Boot failure"
Main_1: PUSH    CS
        POP     DS
        MOV     AL,DS:FATs              ;┐ AX←
        CBW                             ;┘ FAT 数目
        MUL     WORD PTR DS:S_1FAT      ;┐
        ADD     AX,DS:S_1Part           ; │ AX←根目录的起始扇区号
        ADD     AX,DS:Resv_Sect         ;┘
        MOV     DS:Dir_Area,AX          ; 保存根目录的起始扇区号
        MOV     DS:Sectors,AX           ;┐
        MOV     AX,0020H                ; │
        MUL     WORD PTR DS:Directory;  │
        ADD     AX,01FFH                ; │ 文件区起始扇区号→Sectors
        MOV     BX,0200H                ; │
        DIV     BX                      ; │
        ADD     DS:Sectors,AX           ;┘
        CALL    Sys_Check               ; 检查磁盘上是否有 DOS 系统
        JNC     Main_2                  ; 有 DOS 系统
        INT     19H                     ; (无 DOS 系统)更换磁盘, 重新引导
Main_2: MOV     AX,DS:Sectors           ;┐ 文件区起始扇区号(IBMBIO.COM
        MOV     DS:SectorBIO,AX         ;┘ 的起始扇区号)→SectorBIO
        MOV     AX,0070H                ;┐
        MOV     ES,AX                   ; │
        MOV     DS,AX                   ; │
        MOV     BX,0                    ; │
Main_3: MOV     AX,CS:Sectors           ; │
        CALL    Pre_Read                ; │
        MOV     AL,BYTE PTR CS:S_1Track
        SUB     AL,CS:SectorNo          ; │
        INC     AL                      ; │
        XOR     AH,AH                   ; │ 将 IBMBIO.COM 读到 0070H:0
        PUSH    AX                      ; │
        MOV     AH,2                    ; │
        CALL    Read_Disk               ; │
        POP     AX                      ; │
        JC      Main_7                  ; │
```

```
        SUB     CS:BIO_Len,AL           ;|
        JBE     Main_4                  ;|
        ADD     CS:Sectors,AX           ;|
        MUL     WORD PTR CS:Byte1Sect;  |
        ADD     BX,AX                   ;|
        JMP     Main_3                  ;┘
Main_4: PUSH    CS
        POP     DS
        INT     11H                     ; 取系统配置情况
        ROL     AL,1                    ;┐
        ROL     AL,1                    ;|
        AND     AX,3                    ;| CX←软盘驱动器数目
        JNZ     Main_5                  ;| AX←系统引导驱动器
        INC     AX                      ;|     的部件号
Main_5: INC     AX                      ;|
        MOV     CX,AX                   ;┘
        TEST    DS:DrvNo,80H            ; 是用硬盘进行系统引导吗?
        JNZ     Main_6                  ; 用硬盘进行系统引导
        XOR     AX,AX                   ; (用软盘引导)取引导驱动器的部件号为0
Main_6: MOV     BX,DS:SectorBIO         ; BX←IBMBIO.COM 的起始扇区号
        DB      0EAH                    ;┐ 转 IBMBIO.COM 的初始化代码去执行
        DW      0                       ;| (这3条语句相当于1条长转移语句:
        DW      70H                     ;┘  JMP 0070H:0000)
Main_7: MOV     SI,OFFSET BootFail      ;┐ 显示:
        CALL    PutString               ;┘ "Disk Boot failure"
Main_8: JMP     Main_8                  ; 死循环
Main    ENDP
; 显示 ASCIIZ 字符串
PutString PROC  NEAR
        LODS    CS:NonSysDsk            ; 从 ASCIIZ 串中取出1字符
        AND     AL,7FH                  ; 字符串结束否?
        JZ      S_C_2                   ; 字符串结束,返回主程序
        MOV     AH,0EH                  ;┐
        MOV     BX,7                    ;| 显示1个字符
        INT     10H                     ;┘
        JMP     PutString               ; 继续
PutString ENDP
; 检查磁盘上是否有 DOS 系统
; 出口参数: CF=0(有 DOS 系统); CF=1(无 DOS 系统,或读磁盘时出错)
```

```
Sys_Check PROC    NEAR
          MOV     AX,0050H                ;┐
          MOV     ES,AX                   ; │
          PUSH    CS                      ; │
          POP     DS                      ; │ 将根目录的第1扇区
          MOV     AX,CS:Dir_Area          ; │ 读到 0050H:0000
          CALL    Pre_Read                ; │
          MOV     BX,0                    ; │
          MOV     AX,0201H                ; │
          CALL    Read_Disk               ;┘
          JC      S_C_3                   ; 读磁盘时出错
          XOR     DI,DI                   ;┐
          MOV     CX,11                   ; │
S_C_1:    OR      BYTE PTR ES:[DI],20H    ; │ 以小写字母形式表
          OR      BYTE PTR ES:[DI+20H],20H ; │ 示文件名和扩展名
          INC     DI                      ; │
          LOOP    S_C_1                   ;┘
          XOR     DI,DI                   ;┐
          MOV     SI,OFFSET BIO_Name      ; │ 检查磁盘上的第1个文
          MOV     CX,11                   ; │ 件是否为 IBMBIO.COM
          CLD                             ; │
          REPE    CMPSB                   ;┘
          JNE     S_C_3                   ; (不是 IBMBIO.COM)没有 DOS 系统
          MOV     DI,0020H                ;┐
          MOV     SI,OFFSET DOS_Name      ; │ 检查磁盘上的第2个文
          MOV     CX,11                   ; │ 件是否为 IBMDOS.COM
          REPE    CMPSB                   ;┘
          JNE     S_C_3                   ; (不是 IBMDOS.COM)没有 DOS 系统
S_C_2:    RET                             ; 有 DOS 系统，以 CF=0 返主
S_C_3:    MOV     SI,OFFSET NonSysDsk     ;┐ 显示提
          CALL    PutString               ;┘ 示信息
          MOV     AH,0                    ; 等待键盘输入
          INT     16H
          STC                             ; 置 CF，表示无 DOS 系统，或读磁盘时
                                          ; 出错
          RET
Sys_Check ENDP
; 读磁盘前的准备工作(完成逻辑扇区到物理地址间的转换)
; 入口参数：AX=待读的起始绝对扇区号
```

```
Pre_Read  PROC    NEAR
          PUSH    DS
          PUSH    CS
          POP     DS
          XOR     DX,DX                   ;┐
          DIV     WORD PTR DS:S_1Track    ; │SectorNo←处于某
          INC     DL                      ; │ 一磁道中的扇区号
          MOV     DS:SectorNo,DL          ;┘
          XOR     DX,DX                   ;┐
          DIV     WORD PTR DS:DiskSide    ; │ 磁头号→Head
          MOV     DS:Head,DL              ; │ 磁道号→TempUnit
          MOV     DS:TempUnit,AX          ;┘
          POP     DS
          RET
Pre_Read  ENDP
; 读磁盘
; 入口参数: AH=2, AL=待读的扇区数, ES:BX=缓冲区
Read_Disk PROC    NEAR
          MOV     DX,CS:TempUnit          ;┐
          MOV     CL,6                    ; │
          SHL     DH,CL                   ; │CH←磁道号
          OR      DH,CS:SectorNo          ; │CL←扇区号
          MOV     CX,DX                   ; │
          XCHG    CL,CH                   ;┘
          MOV     DX,WORD PTR CS:DrvNo    ; DH←磁头号; DL←驱动器号
          INT     13H                     ; 读磁盘
          RET
Read_Disk ENDP
;
SectorBIO DW      0                       ; 存放IBMBIO.COM的起始扇区号
NonSysDsk DB      Cr,Lf,"Non-System disk or disk error",Cr,Lf
          DB      "Replace and strike any key when ready",Cr,Lf,0
BootFail  DB      Cr,Lf,"Disk Boot failure",Cr,Lf,0
BIO_Name  DB      "ibmbio  com0"
DOS_Name  DB      "ibmdos  com0"
          ORG     7C00H+01FEH
          DB      55H,0AAH                ; 标志
CodeSeg   ENDS
          END     Start
```