

PC-DOS 操作系统 剖析

张桂平 贾厚光 编著

上海科学普及出版社

PC-DOS 操作系统剖析

张桂平 贾厚光 编著

上海科学普及出版社

内 容 提 要

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 (IBM-BIO.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。

读者对象: 微机用户, 程序员, 大中专院校有关专业师生。

组 稿: 联想计算机集团公司

责任编辑: 胡名正 徐丽萍

封面设计: 毛增南

PC-DOS 操作系统剖析

张桂平 贾厚光编著

上海科学普及出版社出版

(上海曹杨路 500 号 邮政编码 200063)

新华书店上海发行所发行 上海印刷七厂一分厂印刷

开本 787×1092 1/16 印张 28.5 字数 687000

1991 年 5 月第 1 版 1991 年 5 月第 1 次印刷

ISBN 7-5427-0540-7/TP·105 定价: 20.00 元

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 操作系统剖析》, 以下简称《剖析》。

《剖析》, 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。

《剖析》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。

《剖析》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《剖析》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
1991年

5354/03

目 录

第一章 PC-DOS 的构造及其加载过程	1
第二章 磁盘引导装入程序	6
第三章 基本输入输出系统 (IBMBIO.COM)	12
第一节 IBMBIO.COM 的组成部分及其作用	12
第二节 重要的数据结构	12
第三节 系统配置文件 (CONFIG.SYS)	13
第四节 源程序清单	14
第四章 DOS 核心 (IBMDOS.COM)	76
第一节 IBMDOS.COM 的组成部分及功能	76
第二节 重要的数据结构	76
第三节 内存管理	80
第四节 磁盘缓冲区管理	81
第五节 源程序清单	82
第五章 命令解释器 (COMMAND.COM)	270
第一节 COMMAND.COM 的组成部分及其功用	270
第二节 重要的数据结构	270
第三节 批处理	271
第四节 DOS 的 EXEC 功能	273
第五节 利用 INT 2EH 执行内部命令和外部命令	274
第六节 源程序清单	275
附 录 软件中断和功能调用列表	444

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）。

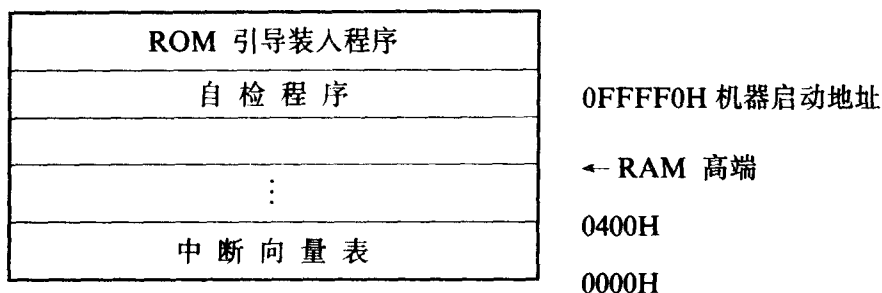


图 1-1

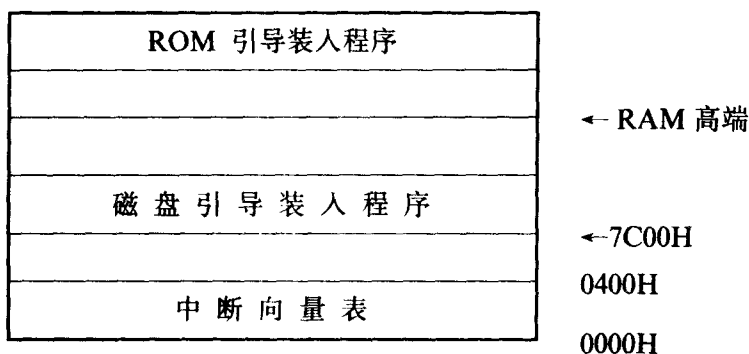


图 1-2

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)。

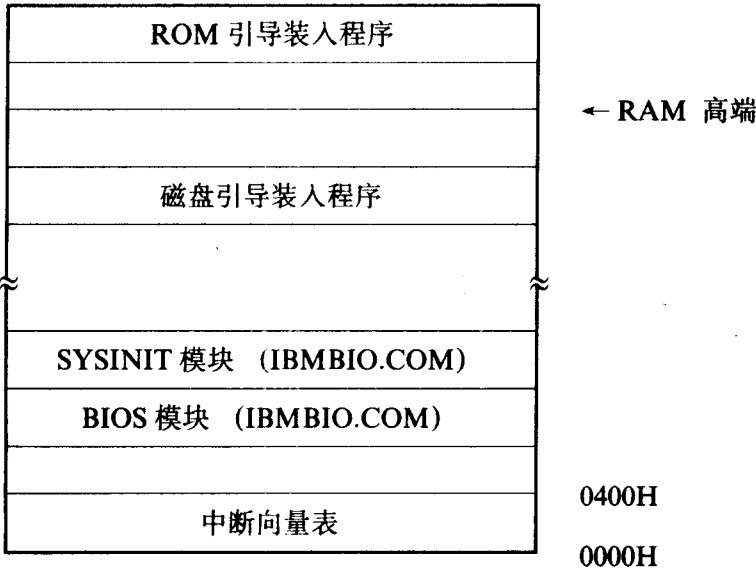


图 1-3

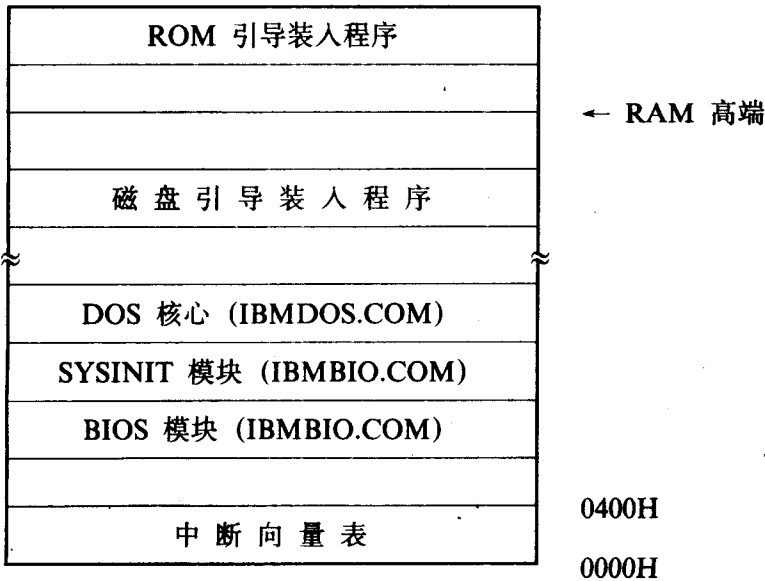


图 1-4

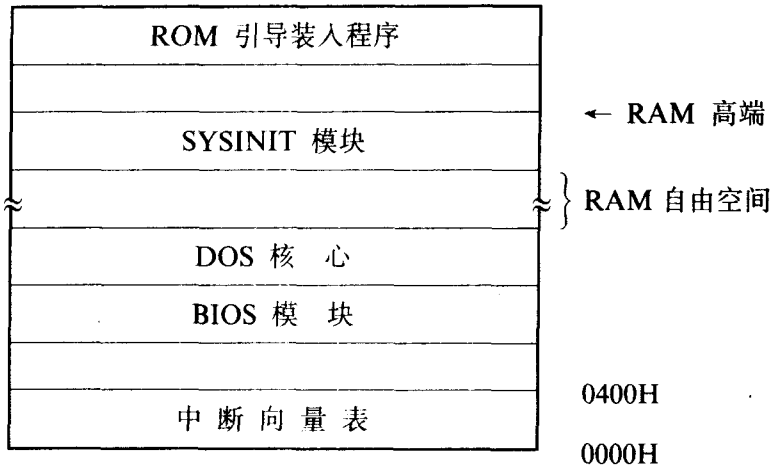


图 1-5

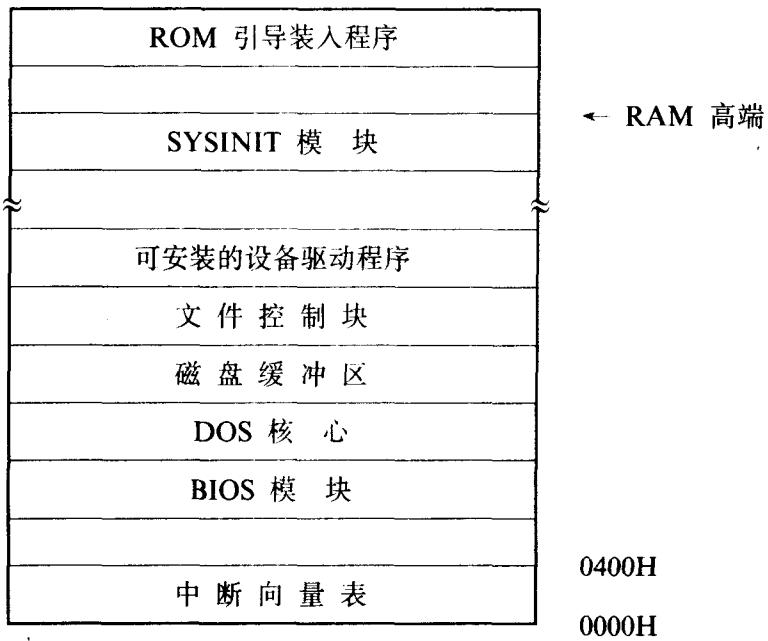


图 1-6

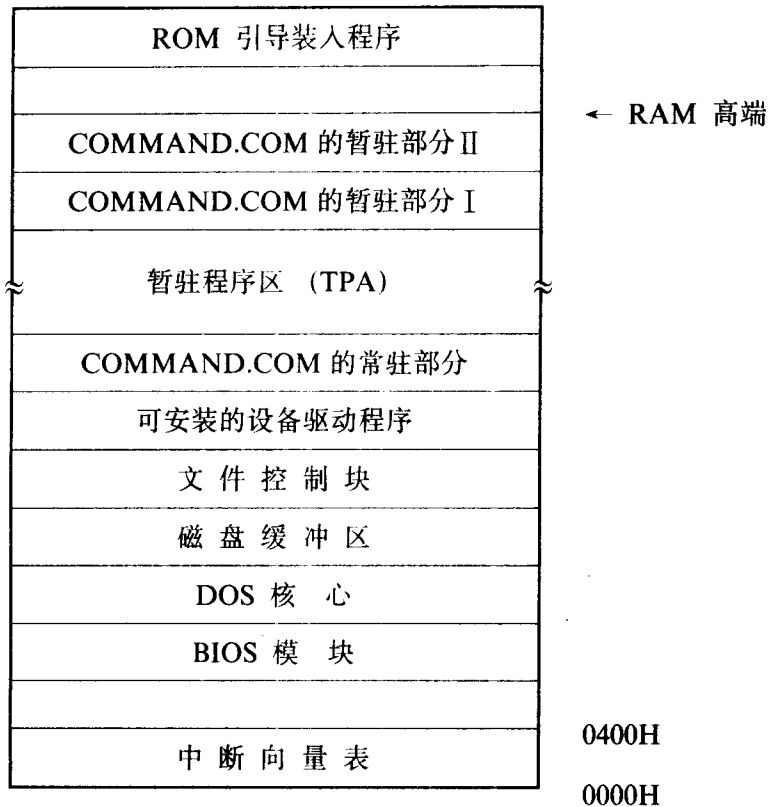


图 1-7

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
BytelSect 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	; 7 AX←
	CBW		; 7 FAT 数目
	MUL	WORD PTR DS: S_1FAT	; 7
	ADD	AX, DS: S_1Part	; 7 AX←根目录的起始扇区号
	ADD	AX, DS: Resv_Sect	; 7
	MOV	DS: Dir_Area, AX	; 保存根目录的起始扇区号
	MOV	DS: Sectors, AX	; 7
	MOV	AX, 0020H	; 7
	MUL	WORD PTR DS: Directory;	7
	ADD	AX, 01FFH	; 7 文件区起始扇区号→Sectors
	MOV	BX, 0200H	; 7
	DIV	BX	; 7
	ADD	DS: Sectors, AX	; 7
	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	; 7 文件区起始扇区号 (IBMBIO.COM
	MOV	DS: SectorBIO, AX	; 7 的起始扇区号)→SectorBIO
	MOV	AX, 0070H	; 7
	MOV	ES, AX	; 7
	MOV	DS, AX	; 7
	MOV	BX, 0	; 7
Main_3:	MOV	AX, CS: Sectors	; 7
	CALL	Pre_Read	; 7
	MOV	AL, BYTE PTR CS: S_1Track	
	SUB	AL, CS: SectorNo	; 7
	INC	AL	; 7
	XOR	AH, AH	; 7 将 IBMBIO.COM 读到 0070H: 0
	PUSH	AX	; 7
	MOV	AH, 2	; 7
	CALL	Read_Disk	; 7
	POP	AX	; 7
	JC	Main_7	; 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 ASCII 字符串
PutString PROC    NEAR
      LODS     CS: NonSysDsk ; 从 ASCII 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

```

第三章 基本输入输出系统 (IBMBIO.COM)

IBMBIO.COM 是系统盘上的第一个文件，其文件属性被特别标识为系统、隐含、只读文件，该文件必须连续存放在磁盘上。

第一节 IBMBIO.COM 的组成部分及其作用

IBMBIO.COM 由两部分组成：BIOS 模块和 SYSINIT 模块。

BIOS 模块的前面部分是驻留的设备驱动程序，包括显示器和键盘驱动 (CON)、宽行打印机驱动 (PRN)、辅助设备驱动 (AUX)、日期和时间驱动 (CLOCK)、磁盘驱动 (块设备)。这些设备驱动程序是操作系统中控制硬件的模块，用于将连接到中央处理器的不同外部设备的特性和操作系统的高层隔离开。DOS 核心 (IBMDOS.COM) 通过 I/O 请求包与这些设备驱动程序进行通信。

BIOS 模块的后面部分是初始化代码。它的作用是：建立磁盘参数表入口；对列表设备和辅助设备初始化；为软盘和硬盘 (块设备) 建立 BPB；将 DOS 核心 (IBMDOS.COM) 读入到内存。初始化代码执行完后，被 DOS 核心所覆盖。

SYSINIT 模块的作用是：将 IBMDOS.COM 进行重定位；调用 IBMDOS.COM 的初始化代码完成一系列的初始化工作 (见第四章第一节)；处理 CONFIG.SYS 文件，设置 DOS 环境；将命令解释器 (缺省的命令解释器是 COMMAND.COM) 读入内存，然后将控制权转交给命令解释器。

第二节 重要的数据结构

一、BIOS 参数块 (BPB)

BPB 是块设备所特有的。BPB 的结构如下：

字节 0—1	每扇区的字节数
字节 2	每簇扇区数 (必为 2 的幂次)
字节 3—4	保留的扇区数
字节 5	文件分配表 (FAT) 的数量
字节 6—7	根目录项的最大数目
字节 8—9	扇区总数
字节 10	介质描述字节
字节 11—12	1 个 FAT 所占的扇区数
字节 13—14	每磁道的扇区数
字节 15—16	磁头数