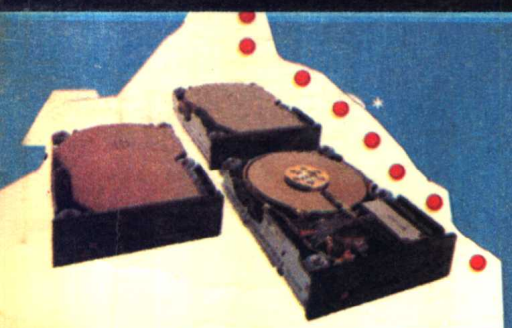
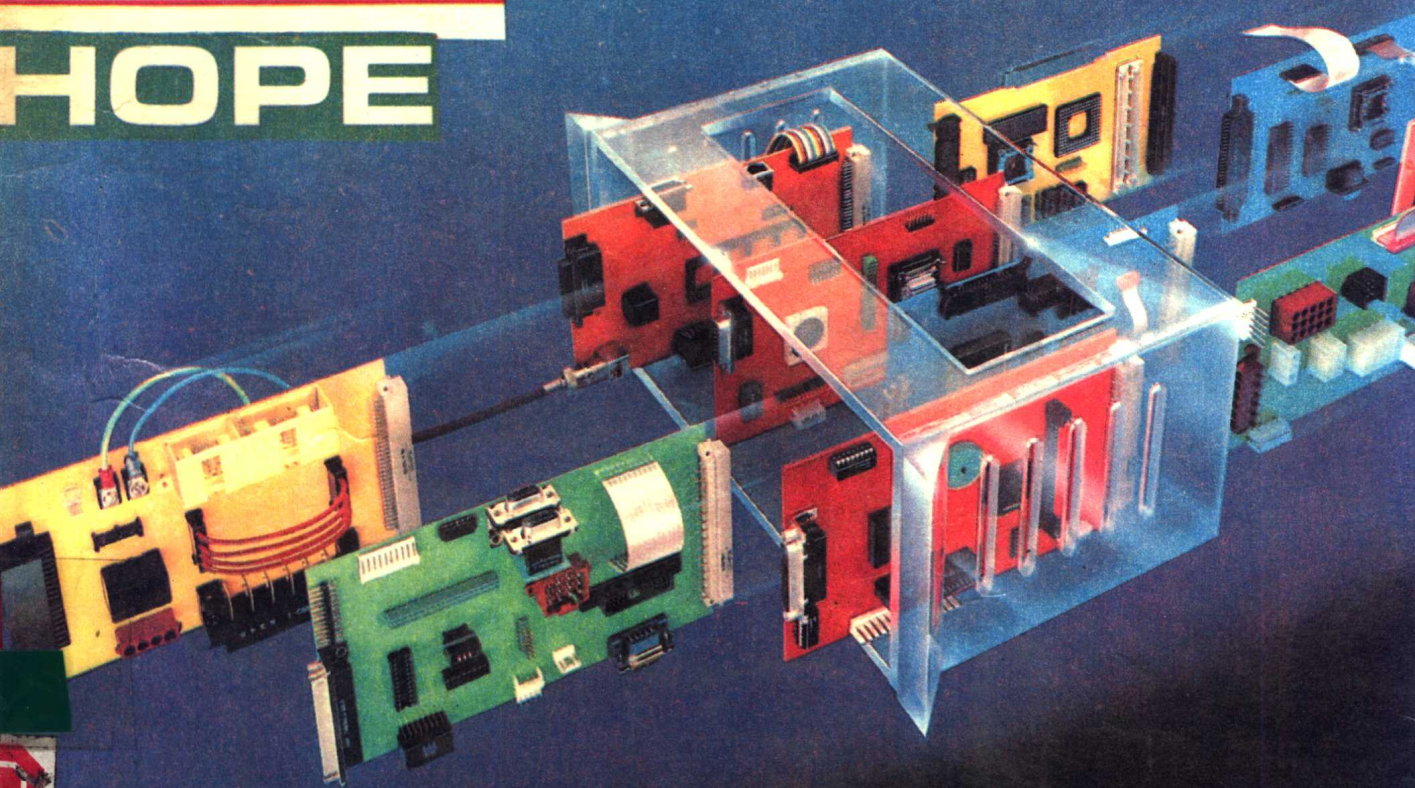
磁盘系统结构与分析流程图

（MS—DOSV2.10—3.20版）



- MS—DOS的结构与初始化
- IO.SYS与MSDOS.SYS的关系
- INT21H的各个功能调用及中断的分析与流程图
- 应用实例
- 分析MS—DOS系统的程序等

HOPE



中国科学院希望高级电脑技术公司

磁盘系统结构
与
分析流程图

（MS—DOSV2.10—3.20版）

乌托什　编译

- MS—DOS的结构与初始化
- IO.SYS与MSDOS.SYS的关系
- INT21H的各个功能调用及中断的分析与流程图
- 应用实例
- 分析MS—DOS的[illegible]程序等

中国科学院希望高级电脑技术公司
一九九一年元月

■ 北京市新闻出版局
准印证号：891430
■ 订购单位：北京8721信箱资料部
■ 邮　　码：100080
■ 电　　话：2562329
■ 传　　真：01—2561057
■ 乘　　车：320、332、302路
车至海淀黄庄下车
■ 办公地点：希望公司大楼一楼
往里走101房间

前　言

当前，国内PC机用户已达几十万，在上面开发的各种软件更是成千上万。对于广大软件工作者来说，工作中最大的困难往往来自于缺乏对系统的了解，而目前有关DOS操作系统的分析资料寥寥无几，因此使得许多软件开发工作难以进行。为了满足大家的需要，我将最近日本出版的由幸田敏记先生所著的《MS—DOS的结构与分析流程》与自己在DOS方面的研究体会结合起来，编译成此书，奉献给各位朋友，愿它能助您一臂之力。

本书的分析以MS—DOS 2.11版本为主，兼顾3.××版本，很多地方与3.×× 版本进行了比较。全书共分为六章，第一章主要介绍了MS—DOS的结构与初始化；第二章介绍了IO.SYS与MSDOS.SYS的关系；第三章是重要也是最精采的一章，它主要介绍了INT 21H的各个功能调用，包括系统保留未公开的调用，还包括其它几个中断的分析。每一个功能模块都有分析流程图与之对应。对MSDOS.SYS的整体也作了深入的分析。第四章主要介绍了一些应用实例；第五章介绍了一些用于MS—DOS系统分析的程序。书中还对MS—DOS涉及到的数据结构做了详尽的分析，这一点是非常重要的。

写作得到了美国Microsoft公司支持，因而具有相当的权威性。

在学习本书时，除了仔细阅读，认真理解外，还应多上机操作实习。可用DEBUG程序来调试有关内容，以便对本书介绍的内容有一个更为全面，深入的认识。

在以往的工作中，曾得到中国科学院软件研究所陈树仁老师的热情关心和帮助及其在业务上的很多指导，对此表示衷心的感谢。还要感谢软件所张尤腊老师以及贾耀梅老师、江一凡老师。在与周宗扬，高泓，汪霞，常成等同志的合作中。学到了很多知识。这是我很难忘的。最后，感谢我的北航校友张亦明同志。对希望电脑公司高效率的工作作风和热情诚恳，治学严谨的工作态度表示钦佩。

由于本人工作经验及日语水平有限，更兼时间仓促，工作繁重，难免出现错误，敬请读者原谅。

编译者

目　录

第一章　系统结构与初始化

1.1 MS—DOS的概要

MS—DOS操作系统分成以下三个部分，即：

IO.SYS

MSDOS.SYS

COMMAND.COM

这三个文件被存放在系统盘上。IO.SYS和MSDOS.SYS是隐含文件（即文件属性是隐含的），因此用DIR指令无法看到。

这几个系统程序是在系统开始时（按复位键）顺序被装载到内存里。系统装载结束后，有关内存的配置见图1.1。

下面是各个程序的大致说明

①IO.SYS

它主要用来控制硬件的操作。象利用通道进行直接I/O（Input/output）存取，是通过使用ROM—BIOS来实现的，IO.SYS是硬件和MSDOS.SYS之间的接口。

具体如软盘和硬盘的输入输出等。

还包括控制台假名汉字的变换，即包含日语输入的功能。

IO.SYS是OEM设计的，PC-9800系列是NEC设计的。

②MSDOS.SYS

是MS-DOS系统的内核部分。主要是支持INT 21H的功能调用。即通过COMMAND COM和外部指令得到功能调用，通过功能调用去调用IO.SYS。

IO.SYS的处理是通过命令包实现的，也就是不能直接处理与逻辑设备码、物理扇区等硬件的关系。命令包与具体设备的驱动程序相联系。MSDOS.SYS包含诸如根据文件名打开文件、关闭文件等操作。它是比IO.SYS高一层的接口。

对于各种机器所使用的MSDOS.SYS，如果版本号相同，则MSDOS.SYS的结构与功能也基本相同。因此本书所分析的MS-DOS可作为其他使用各种类型MS-DOS用户的参考。

标准框功能（template）也在MSDOS.SYS内处理。

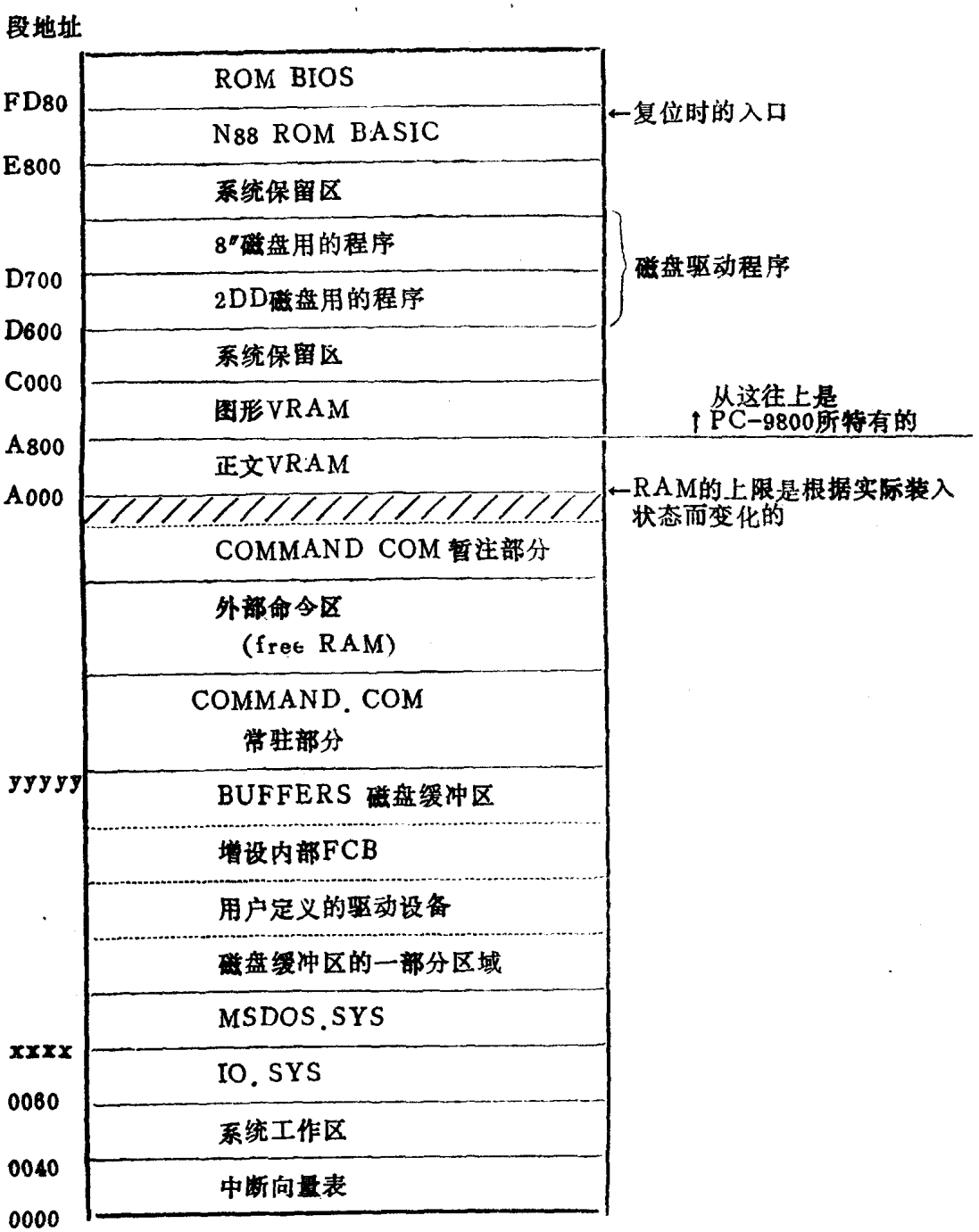
③COMMAND.COM

执行并处理从控制台输入的指令。所谓内部指令是指在COMMAND.COM中的子程序，它不象外部指令那样要从磁盘上装载到内存后，才能加以执行。

COMMAND.COM的常驻部分与非常驻部分在内存中的分配位置见图1.1。常驻部分包括致命的错误处理程序和外部指令执行程序，非常驻部分是再输入子程序。

内部指令集中在COMMAND.COM的非常驻部分。

对于批处理，管道（pipe）处理，环境等也都支持。



IO.SYS的段地址固定在60H

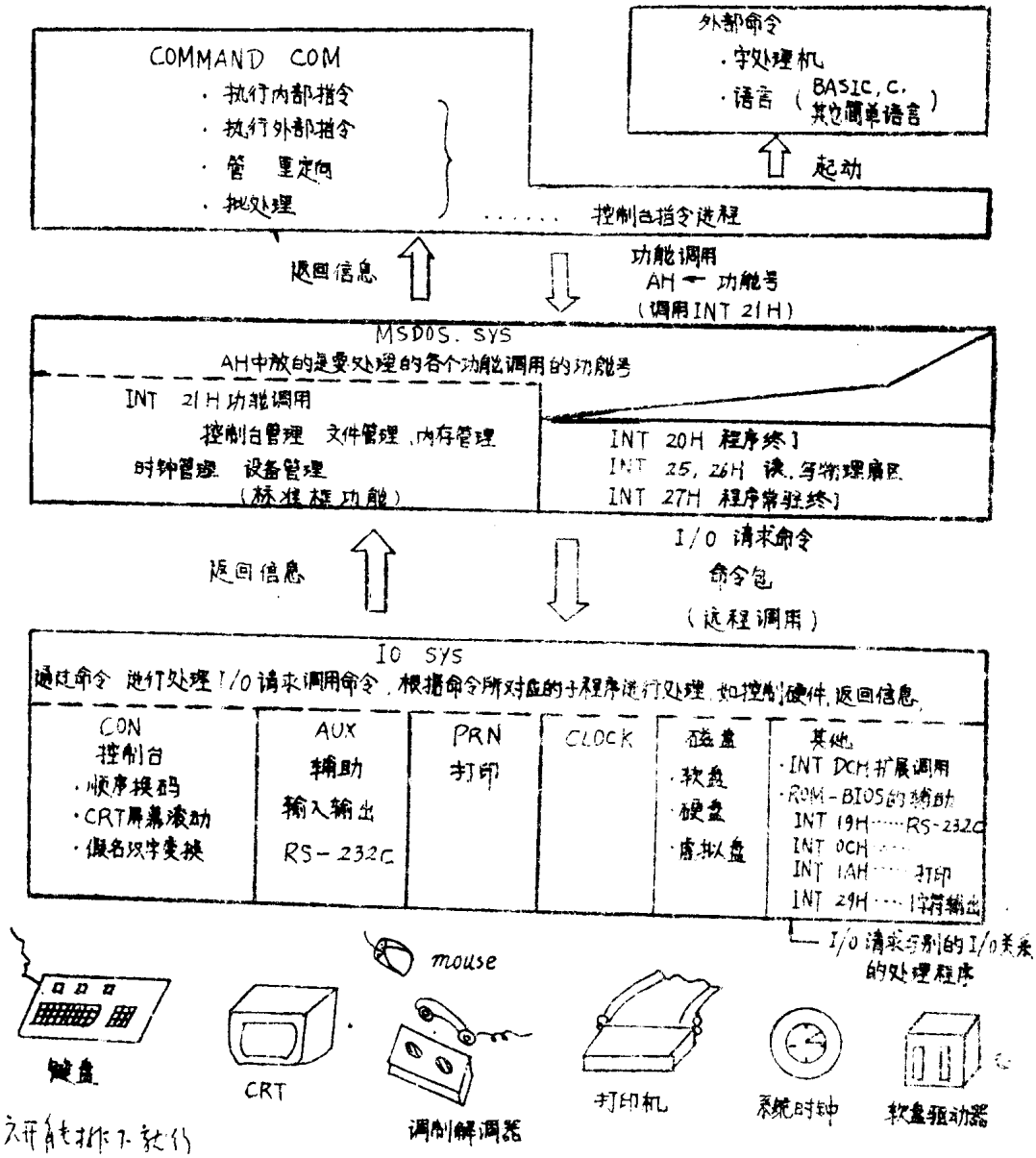
xxxx：MSDOS.SYS的段地址是段0000（0段）86,87H的内容

即INT 21H功能调用的向量的段地址

yyyy：COMMAND.COM的段地址是段0000（0段），位移为BA,BBH的内容

图1.1 MS—DOS系统内存映象

在Ver.2.xx版本基础上改进的各种版本，其整个处理过程和内部指令相似或相同的。



1.2 系统程序间的关系

IO.SYS、MSDOS.SYS、COMMAND.COM之间的数据和指令的联系见图1.2所示

1.2 系统磁盘

系统磁盘的情况见图1.3所示，最初的1扇还是IPL，接下来是FAT，目录，IO.SYS，MSDOS.SYS的程序，最后是使用自由区的程序。存贮在第一个扇区的IPL (Initial Program Loader) 把MS-DOS从准备好的扇区中调入到内存中。

注：在执行外部命令时，如果附加路径名，则FOR命令的内部缓冲区发生溢出，命令处理执行将不正常。

装载有系统的磁盘可以通过执行系统命令，如执行FORMAT.COM/S，就可将系统加载到盘的相应位置上。系统磁盘的目录见图1.4所示，目录内容的顺序是：卷标号，IO.SYS、MSDOS.SYS……或者是IO.SYS、MSDOS.SYS……。其他的文件不是在建立系统盘时登记入目录中的。IO.SYS、MSDOS.SYS的建立过程如上面所说那样，我们已经知道了，通过目录，可以把IO.SYS和MSDOS.SYS程序加载到内存中。

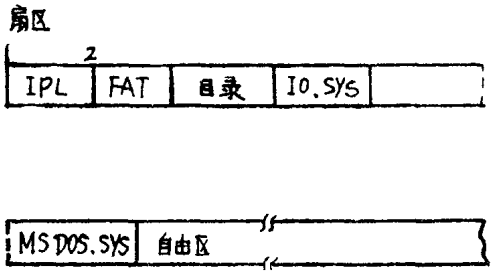


图1.3 系统盘的扇区分配情况

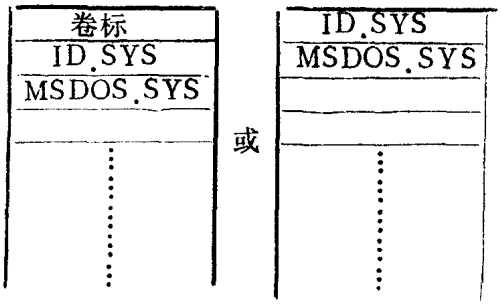


图1.4 系统盘的目录

FORMAT.COM的参数

/S……将缺省驱动器上的DOS软盘中的操作系统文件复制到新磁盘上

/V……给磁盘一个卷标，以便用户用来保持磁盘标记

/9……5″2DD的磁盘被格式化成每个磁道九个扇区，否则每个磁道为8个扇区

8扇区/磁道……全部磁盘容量为640K字节。

9扇区/磁道……全部磁盘容量为720K字节。

（1K字节＝1024字节）

也就是说，每道增加一个扇区，则磁盘容量增加了80K字节。

/C……对FAT和目录的初始化，没有对整个盘面进行实际格式化，这与实际格式化后盘的使用效果相同。因为对整个盘的格式化速度太慢。

/H……硬盘的格式化

/O……在根目录里使用功能调用16H（建立文件）建立文件，根目录里允许建立的文件数目满了以后把它们删除，以检查根目录是否有缺限。

注）卷标是在目录开头部分（2扇区以内）里，也可以没有。见图1.4所示，DIR时可知有无卷标。

若使用FORMAT.COM指令不加/S进行格式化盘，该盘可称之为数据盘。数据盘没有象图1.3所示那样具有IO.SYS，MSDOS.SYS文件。在目录后边便是自由数据区，该区比系统盘的数据区大

因此，如果在驱动器A中插入系统盘，加电后，系统被安装到内存，用户可以工作。如果插入的是数据盘，则在屏幕上返回 'This is the data disk'。系统安装失败，CPU无法继续执行。

1.6 系统开始

MS-DOS系统是从盘中读入到内存中，COMMAND.COM被迅速地起动，等待用户指令的输入

1.3.1 引导装入程序

按动机器的电源开关，接通电源，8086CPU开始工作。首先从FFFF：0000H开始执行，这时除CS寄存器以外的寄存器，其内容都是0000H，对于PC-9801，FFFF：0000H是ROM区（见图1.1）

EA 00 00 80 FD (JMP FAR FD80H：0000H)

首先执行这条指令。FD80：0000H也是ROM区（见图1.1），是ROM BIOS的初始化程序的入口，通过ROM BIOS，执行引导装入程序。

引导装入程序是写在磁盘上的0面，0道，1扇区的IPL程序。它被读到RAM的IFC0：0000H处，这是个远程的开头地址。

1.3.2 IPL (Initial Program Loader)

在系统的0道，1扇区里放的是IPL (Initial Program Loader)。该程序在系统起动时，从盘上把IO.SYS和MSDOS.SYS读入到内存中。IPL的大小通常是1扇区。

IPL分为用于数据盘的IPL和用于系统盘的IPL。

①用于数据盘的IPL

用于数据盘的IPL是'This is data disk'，并在屏幕上的左上角显示出来。同时蜂鸣器报警，CPU停止执行。

②系统盘用的IPL

所准备的磁盘型号（为8英寸型或5英寸型或硬盘）。象NEC公司出品的PC-9801具备8英寸型软盘一个，5英寸2DD型软盘2个（用于8扇区/磁道格式化和用于9扇区/磁道格式化）。另有一个硬盘。

系统盘所用的IPL是：首先把目录头所在扇区读入到内存的0060：0000H处。在目录里记载着IO.SYS和MSDOS.SYS文件的指针。这时候目录的开头是如图1.4所示的那样，可能是卷标号，IO.SYS、MSDOS.SYS，也可能是IO.SYS、MSDOS.SYS。如果都不是的话，系统返回提示"NO System file"。表示引导失败。

IO.SYS，MSDOS.SYS在盘上是连续分配的（如图1.3）。把它们顺序地读入到内存中的以0060：0000H开头的空间中，读入后，在IO.SYS的起始地为0060：0000H中存取的是一条远程调用指令。由该指令跳转到MS-DOS的系统初始化程序。

1.3.3 MS—DOS初始化

把IO.SYS和MSDOS.SYS读入到内存后（见图1.5(a)），通过在IO.SYS头地址内的JMP指令把控制权移交给系统初始化程序。系统初始化就是先由在IO.SYS部分内的初始化程序找到后面的一个记录标题，该记录存放的是CONFIG.SYS解析程序，位于RAM的上限（见图1.5(b)），它也是初始化程序的一部分。

CONFIG.SYS解析程序把MSDOS.SYS向下移动，从而覆盖掉IO.SYS中的系统初始化部分。接下来执行MSDOS.SYS的初始化，假如有CONFIG.SYS文件的话，建立当前PSP，并把它装载到CONFIG.SYS解析程序下面。

这些事情完成后，系统初始化工作还要通过CONFIG.SYS指定驻留的内部缓冲区和内

部FCB。见图1.5(d)

如果内部FCB对应的文件数≤5，则内部FCB所占用的空间可能有部分被其他程序所占用。如在IO.SYS开头里缺省的内部FCB（CON、PRN、AUX、用户使用的FCB等等）。

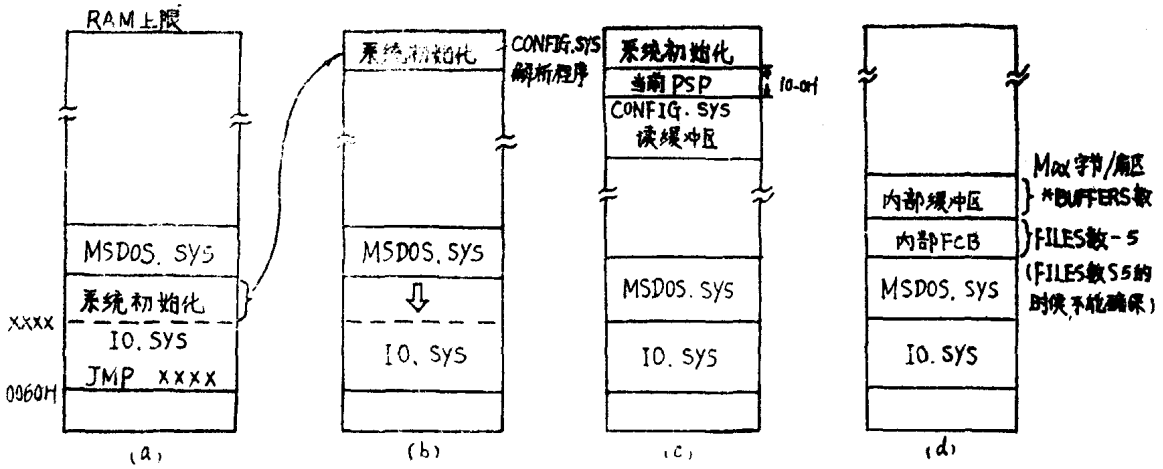


图1.5 系统初始化

CONFIG.SYS的分析程序

它可以作由CONFIG.SYS指定同时打开的文件数等工作。由CONFIG指定的项目有以下几种，其中（ ）内是缺省值。

BUFFERS……磁盘缓冲区数（2）

BREAK……每次功能调用时进行^C的检查（OFF）

SHELL……指令执行过程的路径名的设定（¥COMMAND）

DEVICE……用户驱动设备的设定（无缺省值）

FILES……同时打开的文件数（5）

COUNTRY……国家编码的指定（日本＝81）

SWITCHAR……指令参数转换的指定（／）

AVAILDEV……允许的CON等设备名（允许）

```
CONFIG.SYS
DEVICE=RAMDISK21.COM 8 3
SHELL = A:¥COMMAND.COM /P
BUFFERS = 10
FILES = 6
```

```
-D0.4F
9F63:0000  44 52 41 4D 44 49 53 4B-32 31 2E 43 4F 4D 00 38   DRAMDISK21.COM.8
9F63:0010  20 33 0D 0A 53 41 3A 5C-43 4F 4D 4D 41 4E 44 2E    3..SA:¥COMMAND.
9F63:0020  43 4F 4D 00 2F 50 0D 0A-42 31 30 00 0A 46 36 00   COM./P..B10..F6.
9F63:0030  0A 2F 50 0D 0A 42 55 46-46 45 52 53 20 3D 20 31   ./P..BUFFERS = 1
9F63:0040  30 0D 0A 46 49 4C 45 53-20 3D 20 36 0D 0A 1A 00   0..FILES = 6....
```

DEVICE　SHELL　BUFFERS　FILES

未转换成内部码的部分

图1.7 CONFIG.SYS文件内容转换成内部码实例

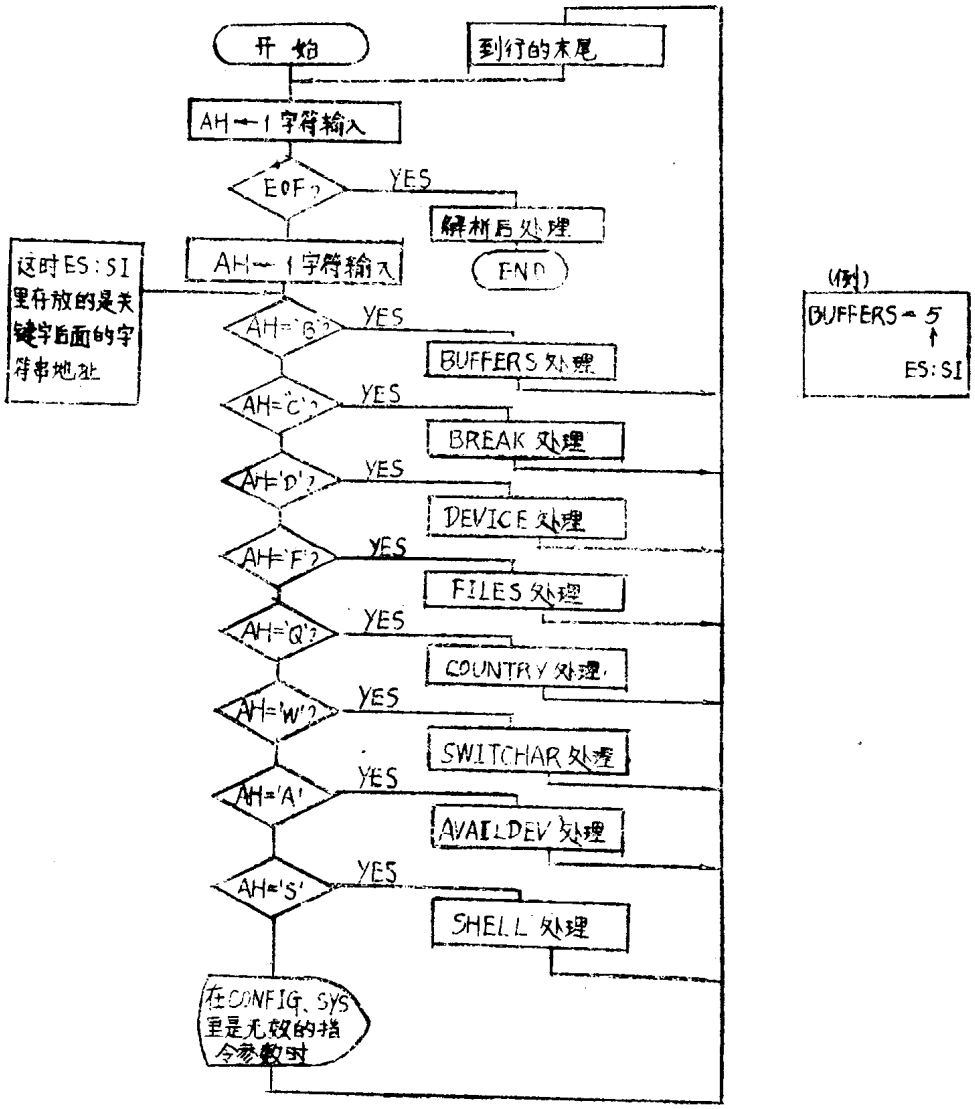


图1.6 CONFIG.SYS关键字的处理

这个时候的SWITCHAR和AVAILDEV，没有发表它们具有的功能（注：MS-DOS 3.0版本以上的版本中，SWITCHAR和AVAILDEV被取消了）。

读入到内存的关键字被转为内部码。内部码用1个英文字母表示。关键字和内部码的对应关系如下：

关键字	内部码
BUFFERS	B
BREAK	C
SHELL	S
DEVICE	D
FILES	F
SWITCHAR	W

AVAILDEV	A
COUNTRY	Q

根据内部码进行具体处理的关系请见图1.6所示，图1.7表示实际的CONFIG.SYS文件的内容与内部码的变换结果的对应关系及实例。这些内容在系统开始后，驻留在RAM上限附近。

下面是各种处理内容的说明

①BUFFERS处理

把关键字下面的字符串转换成二进制数，数字以外的字符串或缓冲区数大于100〔CONFIG.SYS无效的指令或参数〕，则分析下一行的内容。缓冲区数不到100则保留，为0则可忽略，进行分析下一行。

②BREAK处理

如果关键字下面的字符串是ON，则执行功能AH=33H，DL=1（Break on），并分析下一行。如果是ON以外的字符串不对下一行予以处理（缺省时BREAK=OFF)。即ON以外的字符串全被认为是OFF。

③DEVICE处理

图1.8所示的是DEVICE处理的流程图。把对应设备的BPB，DPB所组成的链读入到内存中的MSDOS.SYS后面。该工作是在初始化时完成的，I/O请求调用是使用MSDOS.SYS的内部程序，在这个初始化时，把如图1.9中的内容存贮在存贮参数的命令包中。（看图1.8)

命令包的（+12～+15H）的内容是把CONFIG.SYS文件读入到内存时候的设备名部分。如果设置了虚拟盘，也可能是所给的虚拟盘大小等的参数。

④FILES处理

把关键字下面的字符串进行十进制→二进制的变换。如果只为0则忽略，转到下一行分析，如果数字超出100〔CONFIG.SYS无效的指令或参数〕也到下一行分析。

在100以下时，把同时打开的文件数存贮起来

⑤COUNTRY处理

把关键字下面的字符串进行十进制→二进制的变换。若是数字以外的字符〔CONFIG.SYS无效的指令或参数〕则转到下一行分析。如果数字是0或大于256也转到下一行分析。

使用功能调用AH=38H，DX=FFFFH（设立国家码）来设置国家码。如果错误〔国家码无效〕也转到下一行分析。

⑥SWITCHAR处理

把关键字参数的一个字符作为转换开关参数的区分记号登记下来。使用功能调用AH=37H，AL=01H（登记转换开关参数）。这个功能调用是未公开的（系统保留)。MS-DOS的版本是3.0以上时，AL=0～2是有效的，但是从CONFIG.SYS中将SWITCHAR已经删除掉了。附带着当AL=0时调用现在的转换开关参数，并把返回值存贮在DL里。缺省值是／（2FH）。关于AL=2，3时将在下面的AVAILDEV中说明。

转换参数是

A>DIR／W

等时，下面是／（2FH)

（注：'／'的ASCII码是2FH)

⑦AVAILDEV处理

如果AVAILDEV=F，则所指定的CON、PRN、AUX、NUL等设备的功能被停止。F以外的则不会。使用功能调用AH=37H，AL=3，DL=0（设备名冻结）。解除（可能使用的设备名）时DL=1。AL=2表示在当前状态下把返回值存贮在DL中。

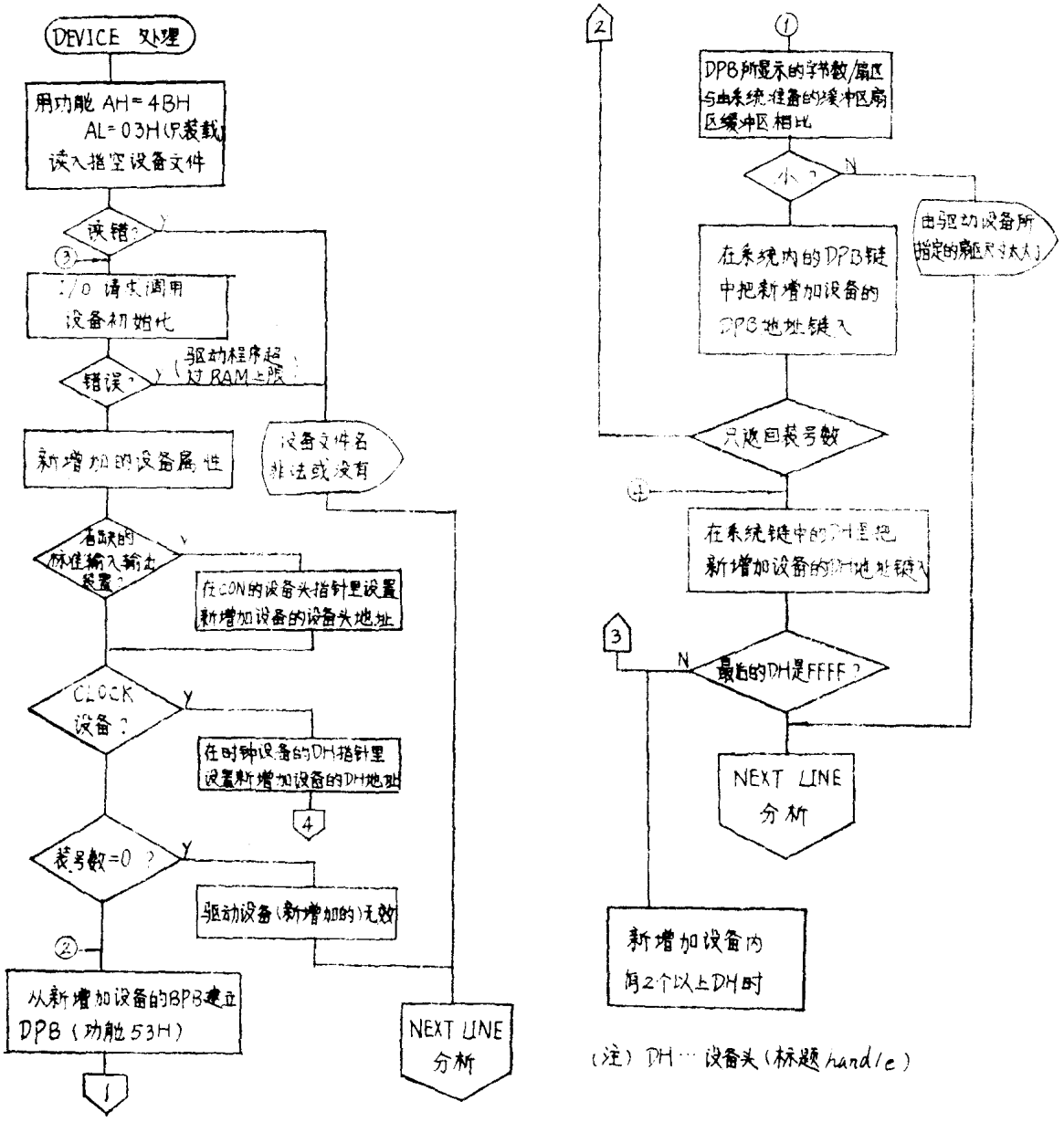


图1.8 DEVICE处理流程图

+0	命令包记录长（这里是16H）字节数
+1	逻辑设备码（这里为0）
+2	指令码（0……初始化）
+3,4	结果状态
+5,+c	保留（系统）
+D	设备数……根据驱动设备设置的
+E～+11	中断地址（驱动设备的END地址）
+12～+15	指向BPB序列的指针……根据驱动设备所设立 指向CONFIG.SYS文件内的DEVICE＝的 参数的指针 即DEVICE＝RAMDISK256 ↑ 指在这里

在指令码中，这部分的构造与大小是相同的（请求标题）

指令码＝0.初始化时的构造

随指令码的不同可发生变化

（关于其他指令请参照第2章第3节I/O请求调用）

图1.9 CONFIG中的DEVICE初始化时命令包的内容

BX	内　容
+0,1	环境段（0000）
+2～+5	指向PSP的80H～FFH的向量
+6～+9	指向PSP的5CH～的向量
+A～+D	指向PSP的6CH～的向量

图1.10，
在通过SHELL起动的命令处理机里所给的参数块

〔使设备名的功能停止〕例如

A>DIR>PRN

结果把目录中的文件打印出来，这意味着已经写入了。

在MS-DOS3.0版本以上的版本已把AVAILDEV从CONFIG.SYS中删除了，因此功能调用AH＝37H，AL＝3也就意义不大了。

⑧SHELL处理

'SHELL＝'后面的字符串，是传送了命令处理程序的文件名。由后面处理起动命令处理程序。如果缺省则系统认为是COMMAND.COM。

把这些命令字符中，在启动命令处理程序时存贮在PSP的80H～FFH里。在后处理的最后部分（参照图1.6），起动命令处理程序是使用功能调用AH＝4BH，AL＝0（程序的装载与执行）来完成的。执行这个程序时，参数块的内容见图1.10所示的表格，这个表的起始地

址存放在DS:BX中。上述指向缓冲区的指针是在存贮在块内的向量。

CONFIG.SYS的SHELL所指定的命令处理程序的环境段地址是0000H，最初的命令处理程序环境段的地址（PSP的2CH，2DH的内容）是0000H。

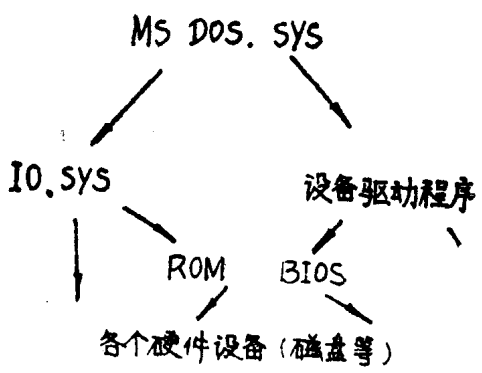
环境是通过命令处理程序管理的。

CONFIG.SYS的分析到此结束了。FILES的值与BUFFERS的值确保了系统工作缓冲区的存在（图1.5(d)）。在开始的时候，根据IO.SYS的构成情况，内部FCB被设置成具有5个文件的数据结构。（0号是AUX,1号是CON、2号是PRN，剩余的2个是用户使用的）•对于内部缓冲区应保证具有的空间为：（磁盘的最大字节数/扇区）*BUFFERS数(字节)。（图1.5（d））

1.3.4 以设备为主的MS-DOS的概要

FCB、BPB、DPB等简略提法曾多次出现，它们在MS-DOS上的位置可见图1.11所示。用户通过控制台直接输入外部命令或COMMAND.COM。每个处理执行都对应着一个PSP用来协调系统与处理接口的关系。处理执行是通过INT 21H的功能调用来执行系统命令。

系统是阶梯形构造



IO.SYS中包含着5英寸软盘和硬盘等的设备驱动程序。还可增设必要的设备驱动程序和新的虚拟盘。IO.SYS和设备驱动程序具有记录入口地址和设备名的设备标题，该设备标题的形式是一个表格。

设备驱动程序开始执行的地址是中断入口。

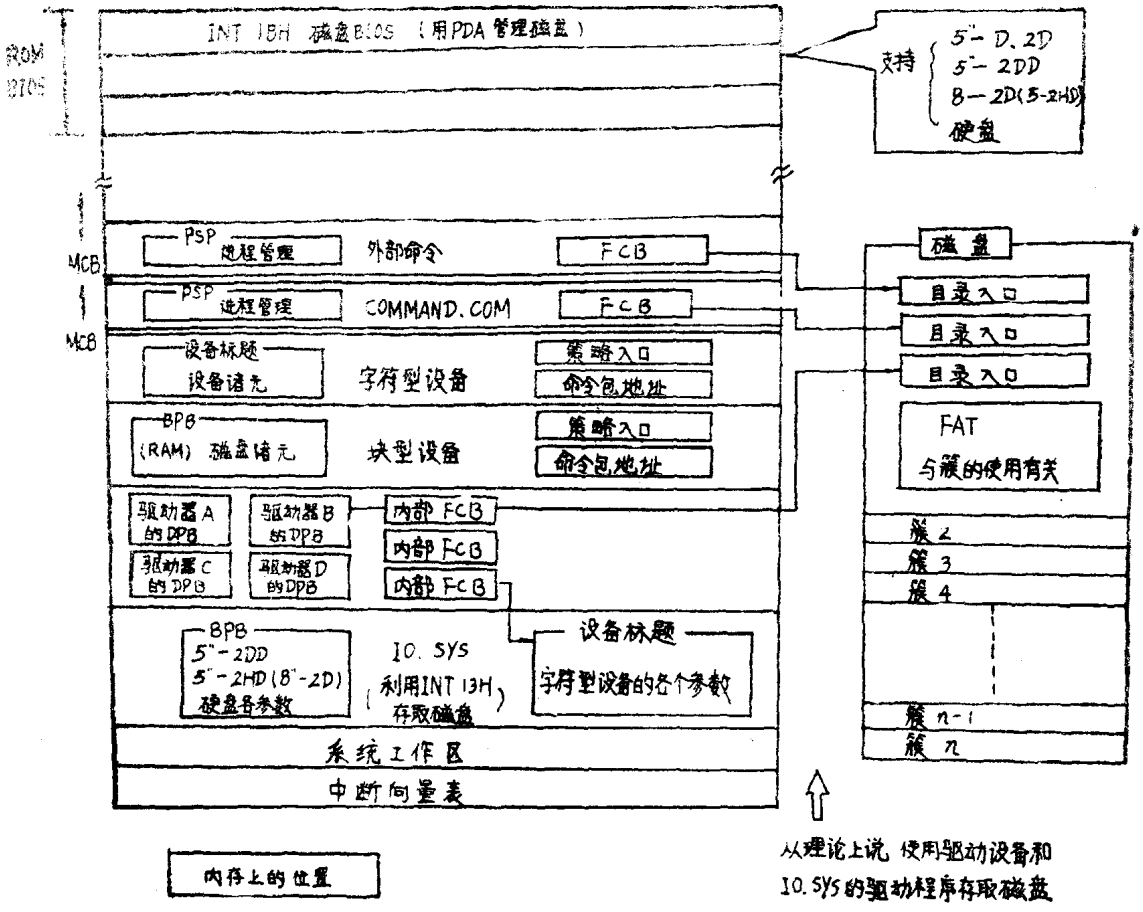
MSDOS.SYS是通过调用中断来向设备驱动程序和IO.SYS发出命令的，其数据是调用策略入口地址，向设备驱动程序传送命令包的地址，通过命令包作各种动作。IO.SYS和驱动设备把关于磁盘（块型设备）的扇区长度是多少字节，FAT数是多少等磁盘参数记在一个被称之为BPB的表中。（看图1.11和图1.12）

MSDOS.SYS检查各个驱动器（A:、B:、C:,……）BPB的各个参量。在各个驱动器的DPB所列举的磁盘参数是通过BPB建立的。DPB里有驱动器数。对于设备驱动程序的或者IO.SYS的BPB里有磁盘的种类数。

在PC 9800系列中，为了存取磁盘，可使用INT 1BH.INT 1BH是用来管理由PDA所描述的磁盘。PDA是对应各个磁盘的号（物理设备地址）。对于相同类型的磁盘则按号被顺序地连接在一起，由命令包所指定的逻辑设备码与PDA是相互对应的。

FCB是分为内部（在MSDOS.SYS内）和外部（通常的FCB）2种，把磁盘上文件或字符型设备对应的信息记录在FCB中。

对于字符型设备是通过FCB所指定的设备名进行存取的。但对于块型设备来说则是通过FCB所指定的目录入口名进行存取的。把FCB中记录着文件本身的信息复制到说明块型设备的目录入口中，当文件信息被修改后，那是需要再往目录入口写一次文件信息。



FCB: FIle Control Block
BPB: Bios Parameter Block
DPB: Device Parameter Block
PDA: Physical Device Address
PSP: Program Segment Prifix
MCB: Memory Control Block

图1.11 系统设备之间的关系及在内存上的分配

1.3.5 COMMAND.COM的初始化

当IO.SYS和MS DOS.SYS的初始化工作完成后，COMMAND.COM就被起动了。COMMAND.COM分成以下三个部分：

①初始化部分

②常驻部分

③暂驻部分

这几部分在内存位置上的分配请见图1.13所示。如果初始化工作完成了，则初始化部分和外部指令区所占用的内存被释放掉。

COMMAND.COM在起动的时候，程序中的起始地址里存放着跳转到初始化部分的JMP指令。执行后，控制权就转交给了初始化程序。