

D O S D O S D O S

DOS

疑难解析

福建科学技术出版社



D O S D O S D O S

(闽)新登字 03 号

内容提要

本书详细叙述了微机上的操作系统 DOS 的各种版本的使用技术问题。主要包括 DOS 的基本概念、DOS 系统的发展、DOS 内部结构分析、DOS 的磁盘布局与文件结构、DOS 批处理程序设计技术、DOS 功能调用及 BIOS 软中断、DOS 内存管理技术、DOS 外部设备管理及其开发环境、DOS 汉化技术等。全书内容深入浅出,将 DOS 的外部功能与 DOS 的内部实现有机地联系在一起,使读者通过本书的学习,能深入地了解 DOS 的奥秘,顺利地解决在使用 DOS 中遇到的各种疑难问题,进而开发出高质量的应用程序和系统程序。

本书可以作为 IBM-PC 及其兼容机用户、程序员、研究开发人员及有关专业人员的技术参考书。

DOS 疑难解析

王晓东 傅清祥

*

福建科学技术出版社出版、发行

(福州得贵巷 59 号)

福建省新华书店经销

福建省科发电脑排版服务公司排版

三日报印刷厂印刷

开本 787×1092 毫米 1/16 24.75 印张 2 插页 624 千字

1995 年 11 月第 1 版

1995 年 11 月第 1 次印刷

印数:1—5 000

ISBN 7-5335-0948-X/TP·28

定价:22.90 元

书中如有印装质量问题,可直接向承印厂调换



IBM-PC 系列微机以其先进的系统结构和丰富的软件资源日益受到我国广大微机用户的信赖。目前在 PC 系列机及其兼容机上运行的 DOS 操作系统是应用最广泛的操作系统。它是微机最核心的系统软件。微机所能提供的所有功能都以 DOS 的基本功能为基础。所以, DOS 的效率和速度,在很大程度上决定了整个微机系统的效率和速度。DOS 又是一个微机用户使用最多的系统软件。任何一个微机用户,从他接触微机的那一瞬间起,就与 DOS 结下了不解之缘。用户对微机的任何一个操作都是通过 DOS 来响应的。DOS 的基本命令简单明了,易于理解、记忆和使用。有一定文化水平的用户,经过短期培训、学习,就能很快掌握 DOS 的使用方法。另一方面, DOS 本身又是一个十分精巧且包含各种计算机技术的系统程序。在广大的微机用户中,只要是对应用有稍高要求的人,都迫切需要了解 DOS 的内部技术。

本书的写作目的有二。其一是作为已初步掌握 DOS 使用方法的用户进一步学习的进阶读物。广大微机用户在使用 DOS 过程中,难免会遇到各种各样的问题,有时,百思不得其解。其中很大一部分的疑难是由于对 DOS 的内部技术不了解或不熟悉造成的。本书力图从原理上阐述 DOS 的组成与工作机理,使读者通过有关章节的学习,从根本上了解 DOS 的有关命令和使用方法,知其然,又知其所以然。这样许多疑难问题就会不攻自破,迎刃而解。其二是为读者提供一部关于 DOS 的比较完整、全面的参考书。对 DOS 提供的各种功能、DOS 的实现原理和方法等方面的资料进行系统、有机的整理,并将 DOS 的外部功能与 DOS 的内部实现有机地联系在一起,既给出 DOS 的功能,又说明如何充分地利用 DOS 提供的功能以及在使用和开发应用程序的过程中遇到问题时应如何寻找解决问题的途径等。

总之,为了使微机用户更深入地了解 DOS,更充分地利用 DOS 的功能,本书结合 DOS 的具体实现及运行机制,为读者提供尽可能详细的资料和尽可能透彻的分析,使读者通过本书的学习,能更深入地了解 DOS 的奥秘,顺利地解决在使用 DOS 中遇到的各种疑难问题,进而开发出高质量的应用程序和系统程序。

本书的各章均以问题为标题,以期明确地提示有关疑难问题应重点阅读的章节。每章内容各自构成一个完整、独立的主题。第一章阐述 DOS 的整体结构与内部组成。第二章涉及 DOS 的文件管理。第三章的内容是关于 DOS 命令的编程。第四章剖析了 DOS 中断调用这一 DOS 的核心技术。第五章的主题是 DOS 的内存管理技术。第六章则涉及 DOS 的外部设备管理。第七章阐述在 DOS 环境中的汉字信息处理技术。读者可以根据自己的需要和兴趣,研读或查阅有关章节的内容。

本书是集体劳动的结晶。其中,第二章和第三章由傅卓文执笔。第一、四、五、六、七章由王晓东执笔。傅清祥教授主审全书。参加本书初稿讨论和编写工作的还有田俊、王梅集、范庆等同志。

由于时间仓促和作者水平有限,难免挂一漏万,书中不当和疏漏之处,望读者不吝斧正。

编著者 谨识

1995 年 10 月

目 录

第一章 什么是 DOS?

——DOS 概述	(1)
§ 1.1 DOS 的基本概念	(1)
§ 1.2 DOS 的发展概况	(2)
§ 1.3 DOS 内部结构分析	(4)
(一) DOS 的引导过程	(5)
(二) DOS 的内存映象与层次关系	(12)
§ 1.4 DOS 命令和应用程序的运行机制	(14)
§ 1.5 常用的 DOS 命令	(23)

第二章 病毒和软件加密是如何利用 DOS 的?

——磁盘布局 and 文件结构	(27)
§ 2.1 磁盘的基本结构	(27)
§ 2.2 DOS 的文件管理	(30)
§ 2.3 病毒的原理	(38)
§ 2.4 软件加密的原理	(40)

第三章 如何用 DOS 命令编程?

——批处理程序设计技术	(46)
§ 3.1 什么是批文件	(46)
§ 3.2 ANSI.SYS 的扩充控制	(58)
§ 3.3 交互式批文件	(65)
§ 3.4 如何创建一个批文件	(68)
§ 3.5 宏 (Macro) 和批文件	(70)

第四章 如何深入 DOS 进行程序设计?

——DOS 中断调用	(72)
§ 4.1 中断向量表	(72)
§ 4.2 DOS 系统功能调用—INT 21H	(74)
§ 4.3 其它常用中断调用	(104)
§ 4.4 DOS 中断调用编程模式	(140)
(一) 用汇编语言调用 DOS 中断	(141)
(二) 用 C 语言调用 DOS 中断	(143)
(三) 用 Pascal 语言调用 DOS 中断	(145)

(四)	用 Quick BASIC 语言调用 DOS 中断	(148)
(五)	截取并修改 DOS 中断	(151)

第五章 如何突破 DOS 640K 内存限制?

	——DOS 内存管理技术	(157)
§ 5.1	PC 机的内存类型及限制	(157)
§ 5.2	常规内存管理	(162)
(一)	内存控制块链	(162)
(二)	程序环境块	(163)
(三)	内存分配过程	(164)
(四)	内存分配块的释放和修改	(165)
(五)	覆盖程序	(167)
(六)	内存驻留程序 (TSR)	(169)
§ 5.3	使用扩展内存	(173)
(一)	扩展内存规范 EMS	(173)
(二)	EMS 工作方式和使用方法	(174)
(三)	EMS 命令	(177)
§ 5.4	使用扩充内存	(190)
(一)	通过 BIOS 访问扩充内存	(190)
(二)	用 XMS 设备驱动程序访问扩充内存	(192)
§ 5.5	内存配置的优化	(202)
(一)	上位内存	(203)
(二)	高速缓存	(205)
(三)	RAM 磁盘	(208)
(四)	打印机假脱机缓存	(210)
§ 5.6	DOS 扩展器	(212)
(一)	80×86 保护方式	(212)
(二)	DOS 扩展器的工作原理	(223)
(三)	DOS 扩展器的使用方法	(226)
(四)	VCPI 与 DPMI	(229)
(五)	DOS 扩展系统功能调用	(233)

第六章 DOS 是怎样管理外部设备的?

	——DOS 环境与设备驱动程序	(247)
§ 6.1	标准设备驱动程序与 DOS 环境	(249)
(一)	DOS 标准设备驱动程序	(249)
(二)	DOS 环境设置	(256)
§ 6.2	块设备	(275)
§ 6.3	可安装设备驱动程序	(287)

(一)	常用的 DOS 可安装设备驱动程序	(287)
(二)	设备驱动程序的结构	(301)
(三)	设备驱动程序的工作原理	(304)
(四)	设备驱动程序的功能及调用格式	(311)
(五)	设备驱动程序设计	(325)
(六)	调试设备驱动程序	(332)
 第七章 在 DOS 中如何使用汉字?		
	——DOS 汉化技术	(335)
§ 7.1	汉字的计算机表示	(335)
§ 7.2	汉字操作系统的组成与内部结构	(339)
§ 7.3	RAM—BIOS 模块结构	(347)
§ 7.4	常用汉字操作系统	(358)
§ 7.5	直接写屏技术与 DOS 内核的汉化	(379)
 附录: DEBUG 主要命令		 (387)

第一章 什么是 DOS?

——DOS 概述

§ 1.1 DOS 的基本概念

DOS (Disk Operating System) 是磁盘操作系统的英文缩写。它由软盘或硬盘提供, 是适用于 IBM-PC 及其兼容机的磁盘操作系统。它负责管理计算机及其所执行的处理过程。DOS 的第一目标是将裸机转换为一台用户易于使用的机器, 也就是说它向用户提供一台虚拟计算机, 其特性不同于作为基础的物理处理机。由于裸机的输入/输出 (I/O) 系统相当复杂, 为了使用它们, 需要进行繁琐的程序设计。而 DOS 则向用户提供了一台具有 I/O 功能且易于使用的虚拟机, 从而解除了用户的沉重负担。除此之外, DOS 还提供了管理其它系统资源以及辅助应用程序的开发和执行的環境。

下面简要介绍 DOS 的主要功能:

执行命令和程序 DOS 对命令和程序的执行, 是用户最先接触到的操作系统功能。DOS 启动后, 在显示器上显示出操作系统的提示符 C> (或 A>), 表示计算机正在等待用户发出命令。用户在提示符后键入命令或程序名, 操作系统立即作出一系列反应: 分析命令或程序名, 从磁盘上查找用户需要的程序并调入内存, 将控制权转交给程序, 运行该程序, 完成用户的要求。程序运行完成后, 控制权又重新转交给 DOS。

内存管理 在执行程序之前, 必须先将程序调入内存。程序在获得足够内存空间之后, 才能运行。DOS 负责对内存资源的管理。在调入程序时, 根据程序的要求为它分配内存空间; 程序运行结束后, DOS 回收已分配的内存空间。

输入/输出设备管理 输入/输出设备是计算机系统的重要组成部分。程序和各种信息都要通过输入设备输入到计算机中; 而计算的结果要输送到输出设备中, 以便显示、打印或保存。常用的输入设备有键盘、鼠标器和数字化仪等。常用的输出设备有显示器 CRT、打印机和绘图仪等。常用的既能输入又能输出的设备有软盘驱动器和硬盘驱动器等。DOS 操作系统相当大的部分用于管理输入/输出设备, 尤其是对显示器、硬盘的输入/输出管理给用户提供了很大的方便。在运行程序时, 用户通过中断调用服务程序访问输入/输出设备。服务程序负责完成数据的传送和设备的检查。如果发生错误, 服务程序将把出错情况告诉用户。

磁盘空间及文件管理 用户的程序和数据是以文件的形式记录在磁盘上的, 在使用时, 由 DOS 负责对文件的存取。通常一个新的磁盘是未格式化的, 使用之前要由 DOS 的格式化程序进行格式化, 否则无法用来记录信息。格式化程序的作用是: 将磁盘划分成磁道和扇区; 在磁盘上建立两个说明磁盘使用情况的表: 磁盘空间分配表、磁盘文件目录表。磁盘空间分配表用于记录自由空间的分布情况和目前已使用的空间分布情况; 磁盘文件目录表用于保存磁盘文件名、文件的大小、占用磁盘空间的起始地址等。这两个表合起来作为管理磁盘的依据。当用户在磁盘中建立新文件时, DOS 首先在磁盘文件目录表中查找该文件, 若未找到, 则将

此新文件名登录在磁盘文件目录表中，然后根据文件的大小分配磁盘自由空间给该文件，将分配结果登录在磁盘空间分配表中，最后把文件信息写入分配的磁盘空间中。当用户删除磁盘文件时，DOS 将从磁盘文件目录中注销该文件名，回收该文件占用的磁盘空间，重新计算磁盘的自由空间，然后将此结果写回磁盘空间分配表中。

§ 1.2 DOS 的发展概况

从DOS的产生到现在已经历了十多年的时间。在这十多年的时间里，DOS 经历了一个不断更新不断完善的过程，几乎每年都有新的DOS版本诞生。最早的DOS版本要追溯到1980年问世的86-DOS。当时，微机上的操作系统多是Digital Research的CP/M操作系统。8088/8086 CPU芯片刚刚问世，86-DOS就是专门为这种芯片设计的。1981年Microsoft买下了86-DOS的所有版权，正式发表了MS-DOS1.0。PC机问世后，Microsoft将DOS的使用权授予IBM，并达成协议：IBM可以发表其DOS版本PC-DOS，但必须保证MS-DOS与PC-DOS在功能上等同。IBM于1981年正式发表了PC-DOS1.0。在此后十多年的发展中，MS-DOS一直与PC-DOS并存，它们的各个版本及源代码都大致相同。

DOS版本的不断更新，固然有不断改正程序错误、不断完善的因素，但更主要的是为了适应硬件的变化。表1.1.1列出的是主要的DOS版本、发表时间以及所作的重大改进。

表 1.1.1 DOS 版本发表时间及所作的改进

版 本	日 期	改 进 功 能
86-DOS	1980	DOS 的早期版本
1.0	1981	支持早期 PC、5.25 英寸* 的单面磁盘
1.1	1982	支持 5.25 英寸的双面磁盘
1.25	1982	第一个 OEM 版本，增加命令 VERIFY
2.0	1983	支持 PC/XT 和硬盘
2.1	1983	支持 PCjr 和 PC 便携机
3.0	1984	支持 PC AT 和高密软磁盘
3.1	1985	支持网络
3.2	1986	支持 3.5 英寸软磁盘
3.3	1987	支持 PS/2
4.0	1988	支持 32M 以上硬盘和 EMS
5.0	1991	支持 XMS、UMB 和 HMA
6.0	1993	支持笔式计算环境和 PCMCIA 卡
6.2	1994	清除 6.0 故障，改进硬盘管理

*：1 英寸=2.54 厘米。为用户方便，本书保留英寸这个计量单位。

十多年来，MS-DOS 与 PC-DOS 在微机操作系统软件市场上独领风骚，但这个市场也不是他们的一统天下，别的操作系统软件也在产生与发展。其中一个令人瞩目的操作系统是 Novell 的 Novell DOS7，其前身是 Digital Research 公司的 DR DOS。Novell 的作法比较独特。

它基本上重写了 DOS 的内核。当然，用户可以得到类似于 MS-DOS 和 PC-DOS 所提供的工具集，但不同的是 Novell DOS 提供了真正的多任务机制，内置了网络功能。用户在 Novell DOS 的基础上再购置一些网络接口卡和电缆，就可以用 Novell DOS 的安装程序将机器连起来构成一个小型的网络。

纵观 DOS 的发展历程，不管是哪一种 DOS 都特别注重以下几个方面并各自有所作为：

1. 兼容性

一般来说，DOS 的兼容性包括以下三个方面：

硬件兼容性 通常 DOS 与硬件具有较好的兼容性。每一个 PC 兼容机制造厂商要在市场上立脚，都必须使自己的硬件符合标准。

命令级兼容性 前述三种 DOS 系统的命令级兼容性不是很好。MS-DOS 从最近的两个版本中去掉的命令如 COMP、DOSSHELL 和 PRINTER.SYS 等至今都还保留在 PC-DOS 中。而 PC-DOS 缺乏大多数 MS-DOS 用户非常喜欢使用的两个程序 EDIT 和 QBASIC。在 PC-DOS 6.1 中有了自己的编辑器和语言解释器。

在某些方面，Novell DOS 走的是自己的道路。例如它的 DIR 命令就没有 MS-DOS 6.0 中的许多扩展功能，如按文件属性列表、排序、列子目录等。对批处理文件的使用方法也有所改变。Novell 认为它的方案在技术上比 Microsoft 的先进，所以用不着刻意去追求兼容。但用户要求的往往是百分之百的兼容。

与现有应用程序的兼容性 与现有应用程序如 Windows 等的兼容性对用户来说是至关重要的，各 DOS 厂家也十分重视，即使是 Microsoft，对每一个升级的 DOS 版本，都要发行成千上万份 beta 软件进行验证，以保证与用户应用程序的绝对兼容。

2. 内存管理

对于一般性的程序及数据，DOS 只承认 640K 的常规内存。这一限制对于 PC 的内存管理是一个严重的障碍，但这对于 DOS 而言又是最基本的，它建立在 DOS 的最核心部分，因而不能将这个限制去掉。到现在为止，各种 DOS 系统都未能突破 640K 的常规内存限制，但已经接近将所有 640K 的常规内存都向用户开放的程度。各种 DOS 都设计了各自的内存管理程序将设备驱动程序(Driver)和其它内存驻留程序(TSR)放到 640K~1M 之间的上位内存(upper memory)中。Novell DOS 甚至可以让内存驻留程序在 1M 以外的扩充内存(extended memory)中运行，但对这些程序的设计提出了一些特殊的要求。

3. 实用程序集

DOS 除了提供对机器操作最基本的功能外，一般都提供一组实用程序(或称为工具)，帮助用户完成对文件、磁盘等的管理。因此，评价一个 DOS 系统对用户是否具有吸引力，很大程度上取决于它所提供给用户的实用程序是否让用户感到满意。

磁盘数据压缩程序 前述三种操作系统的最新版本的磁盘压缩程序都采用了类似的压缩和还原技术，因而其性能，包括压缩比、压缩时间和压缩之后系统性能损失等，基本上是一样的。除了文本文件，三种 DOS 的磁盘压缩程序都未能达到 2:1 的压缩比。MS-DOS 用的是自己的 Double Space。PC-DOS 使用的是 Add Stor 公司的 Super Stor，而 Novell DOS 则使用 Stac Electronic 公司的 Stacker。后两种工具相对 Double Space 来讲有一个显著的优点，

即它们可以压缩软盘上的数据, 让用户能在软盘中存入双倍于软盘容量的数据, 而在一台即使没有安装压缩软件的 PC 机上也照样可以将该软盘上的数据读出来。

文件备份程序 到目前为止, MS-DOS6.2 和 Novell DOS7 都能将文件备份到软盘或由一个驱动器字母指定的设备上, 而 PC-DOS6.1 还能将文件备份到磁带驱动器这个理想的备份介质上。

其它实用程序 三种新版 DOS 都提供了 Undelete 程序, 其功能基本一致。如果没有在磁盘上写入新的数据而破坏已在逻辑上被删去的文件的内容, 则被删去的文件可以很快地得到恢复。反病毒程序第一次使用时首先扫描文件系统并建立一个用于比较的数据库。这个过程一般需要 10 分钟左右。之后的例行检查只需要 1 分钟左右。对于磁盘文件碎片整理程序, MS-DOS 和 PC-DOS 采用的是 Symantec 的产品, 只适用于容量小于 250MB 的硬盘驱动器。而 Novell DOS 则使用其自行开发的程序。

4. 多任务机制

新版的 PC-DOS 和 Novell DOS 都提供了任务切换机制, 允许在同一时间有多于一个的程序处于激活状态。MS-DOS 原来也提供这个功能, 但在 6.2 版本中由于去掉了 DOS SHELL 而丧失了這個功能, 所以在这方面应该说是一个缺陷。PC-DOS6.1 的任务切换是有限制的, 通常在后台的程序在被调到前台之前处于“休眠”状态。Novell DOS7 则跳出了这个框框, 实现了真正的多任务, 允许后台程序在 386 兼容系统中继续运行。Novell DOS7 的另一个独特之处是它的网络功能。它包括了自己的点对点网络软件, 允许用户在没有附加软件的情况下建立一个小型网络。

计算机技术的发展日新月异。伴随着 DOS 的发展, 相继出现了许多新的操作系统。如与 DOS 系统兼容的 Concurrent DOS 和 PC-MOS 等。另外, 一组根本抛弃了 DOS 的操作系统, 如 OS/2、Theos、QNX、Unix 和 Xenix 等, 以全新的面貌崭露头角, 在微机操作系统的市场上与 DOS 争雄。它们完全突破了 DOS 强加给内存的 640K 的限制, 并且可以通过特定的仿真程序运行大部分的 DOS 应用程序。当然, 这些操作系统也有它们自己的限制, 但一般情况下这些限制远远松于 DOS 系统的限制。

展望未来, 虽不敢说 DOS 前程似锦, 但也不是山重水复。由于 DOS 具有众多的用户、众多的工具和应用程序的支持, 随着 DOS 的不断创新和完善, 在将来很长一段时间里, DOS 还不会被其它操作系统所取代, 它仍将是 PC 系列机上最重要的操作系统。

§ 1.3 DOS 内部结构分析

各种版本的 DOS 基本结构是一样的。以 PC DOS 为例, 共有 4 个组成部分:

- 引导程序 (BOOT, 或 IPL)
- IBMBIO.COM (提供系统初始化程序和设备驱动程序)
- IBMDOS.COM (DOS 的核心, 提供 INT21 等中断服务程序)
- COMMAND.COM (提供对于内、外部命令、批命令等的处理)

(一) DOS 的引导过程

从系统加电，到屏幕上出现提示符要经历一段时间，在这一段时间里，系统完成了 DOS 的引导过程。这个过程主要完成以下几项工作：

- 系统加电或复位并自诊断。
- INT19 硬盘自举（或软盘自举）
- 硬盘（或软盘）引导。
- IBMBIO.COM 的初始化。
- IBMDOS.COM 的初始化。
- COMMAND.COM 的初始化。

这些工作，尤其是从读取引导程序（BOOT）起，此后发生的细节对用户是透明的。要深刻地了解规模庞大的 DOS，首先必须弄清完整的 DOS 引导过程。下面分别叙述这几部分的工作过程。

1. 系统加电或复位并自诊断

整个系统的启动流程以读取引导程序为界，可划分为两部分：（开机）→ 自诊断及设备初始化 → 系统初始化 → （出现提示符）。

当系统加电启动时，由电源产生“POWER GOOD”低电位信号，该信号通过 8284A 时钟向 CPU 发送一个 RESET 信号，使 CPU 进入复位状态并强置 CS:IP=FFFF:0000。此时，系统进入 ROM—BIOS 程序区。该区第一条指令为：“CCJMP START”，即跳到硬设备自诊断程序 START 处开始执行。

硬设备自诊断程序是一个长 2K 的固化程序，分别对 CPU、8237 芯片、RAM、8259、8253、显示器、键盘等进行测试，以及初始化软/硬盘、打印机等设备。若检测出致命错误则停机，一般性错误则在屏幕上显示相应的出错信息供用户作进一步的检测并排除错误。当系统诊断无误时，进入自举程序 INT19。需注意的是，在初始化时若检测到硬盘存在，则软盘 I/O 程序由 INT 13 改为 INT 40，而硬盘的 I/O 程序则作为 INT13。另外，INT19 也作了修改，以便将来能进行硬盘自举。这部分的流程图如图 1.3.1。

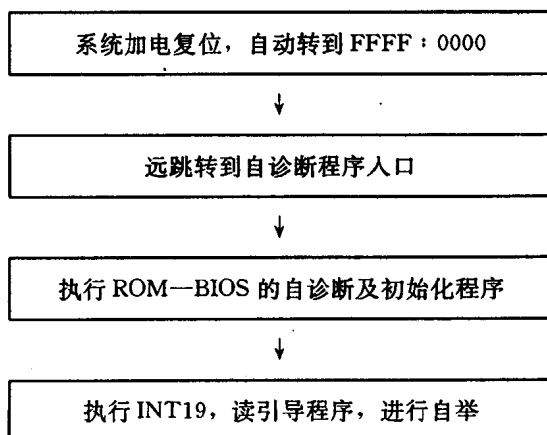


图 1.3.1 系统加电复位自诊断流程图

2. INT19 硬（软）盘自举

对于不带硬盘的系统，DOS 引导程序仅包含 A 盘中 0 面 0 道 1 扇区的 BOOT，而 INT19 只是读出该 BOOT 程序并执行。

对于带硬盘的系统，INT19 中断向量已作了修改以适应硬盘自举。此时情况有所不同。INT19 先读软盘引导程序，不成功再读入并执行硬盘引导程序。对于硬盘来说，DOS 引导程序包括主引导记录及分区 BOOT 两部分。主引导记录执行成功后再读入分区 BOOT 并执行。硬盘的分区 BOOT 与软盘的 BOOT 基本相同，主要差别在于各自的 I/O 参数表不同。

带硬盘系统的自举流程图如图 1.3.2。

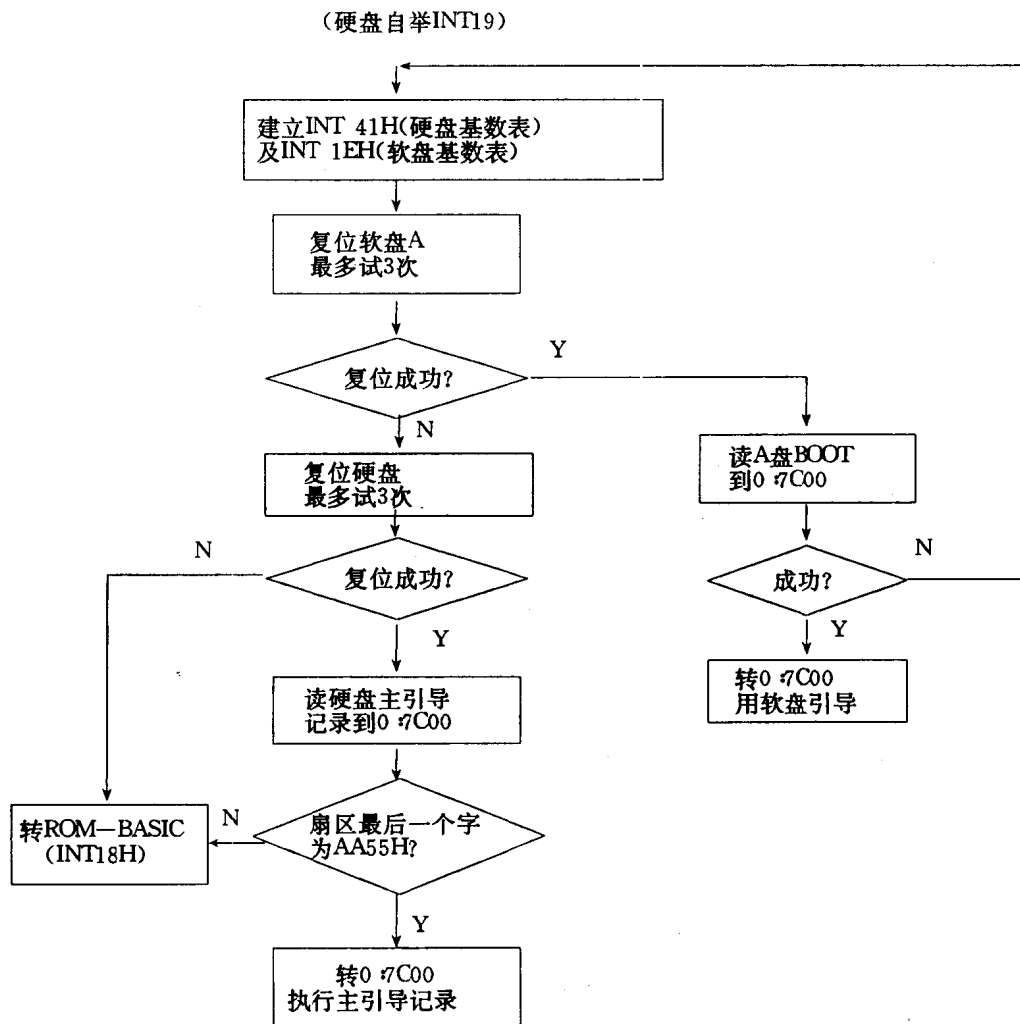


图 1.3.2 带硬盘系统的自举流程图

3. 硬（软）盘引导

系统自举成功后即转入硬（软）盘的 DOS 引导过程。对于硬盘来说，先执行已调入内存 0:7C00 处的主引导记录，检查活动分区（又称“可自举分区”）是否唯一存在，若是则读该分区 BOOT 到 0:7C00 处并执行。

硬盘引导过程的流程图如图 1.3.3。

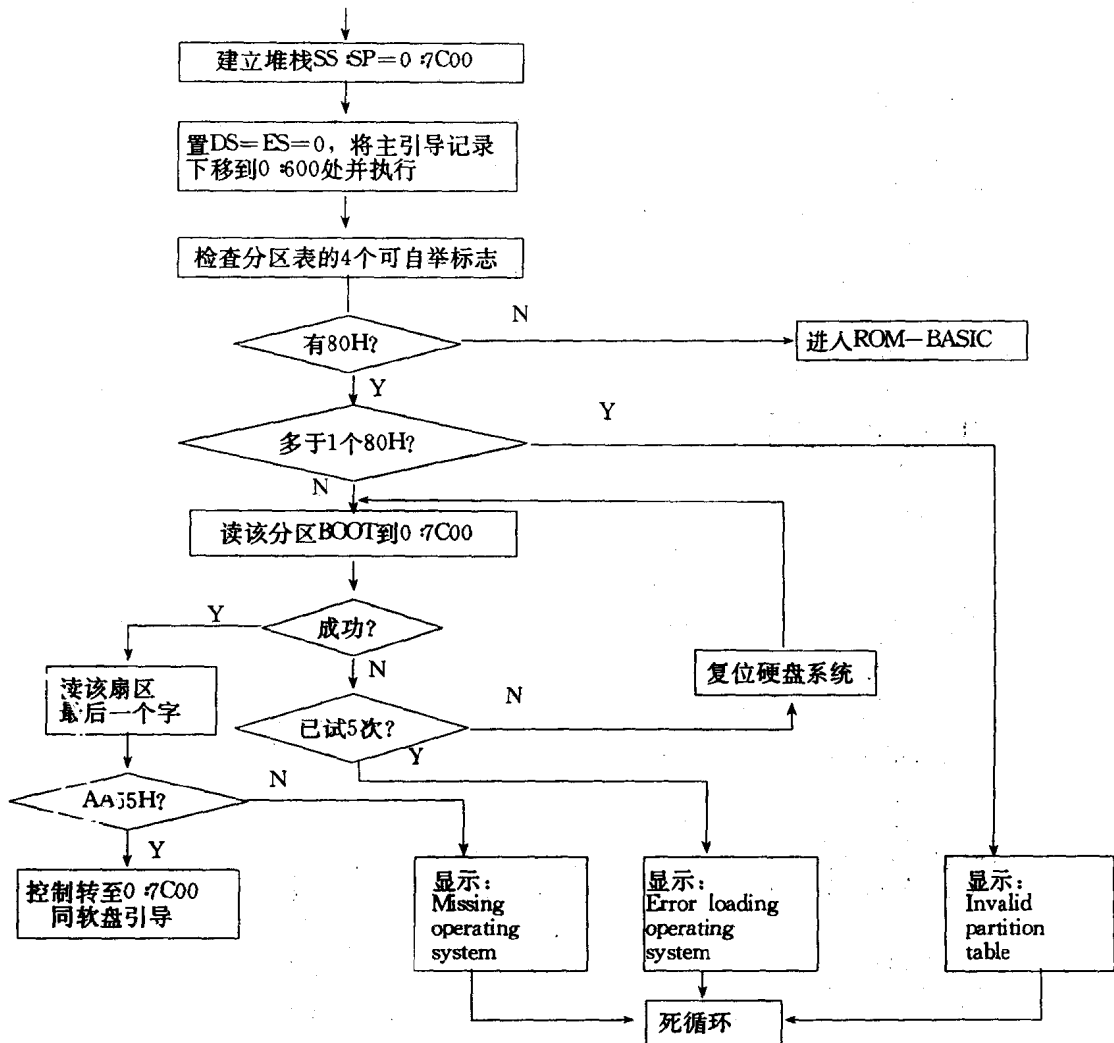


图 1.3.3 硬盘引导过程流程图

系统将软盘 BOOT 或硬盘分区 BOOT 读入内存 0:7C00 后, 引导过程是一致的, 即将控制转到 0:7C00 处执行 BOOT 程序。BOOT 的作用主要是检查 DOS 的头两个文件, 即 IBM-BIO.COM 及 IBMDOS.COM 的存在性。若 IBMBIO.COM 存在, 则它被固定存放在 0070 段, 然后 BOOT 将控制权交给它, 开始 DOS 的启动过程。

BOOT 程序的流程图如图 1.3.4。

4. IBMBIO.COM 初始化

IBMBIO.COM 由两大功能模块组成。第一个模块是系统初始化模块。这个模块又分为 3 个部分, 即: BIO—INIT I、II、III。它们的总长度占了 IBMBIO.COM 的一半以上。第二个模块是常驻内存的接口模块, 作为 ROM BIOS 的扩充部分, 含有控制台驱动、辅助 I/O 驱动、打印机和块设备驱动等程序。

静态的 IBMBIO.COM 文件构成情况如图 1.3.5。

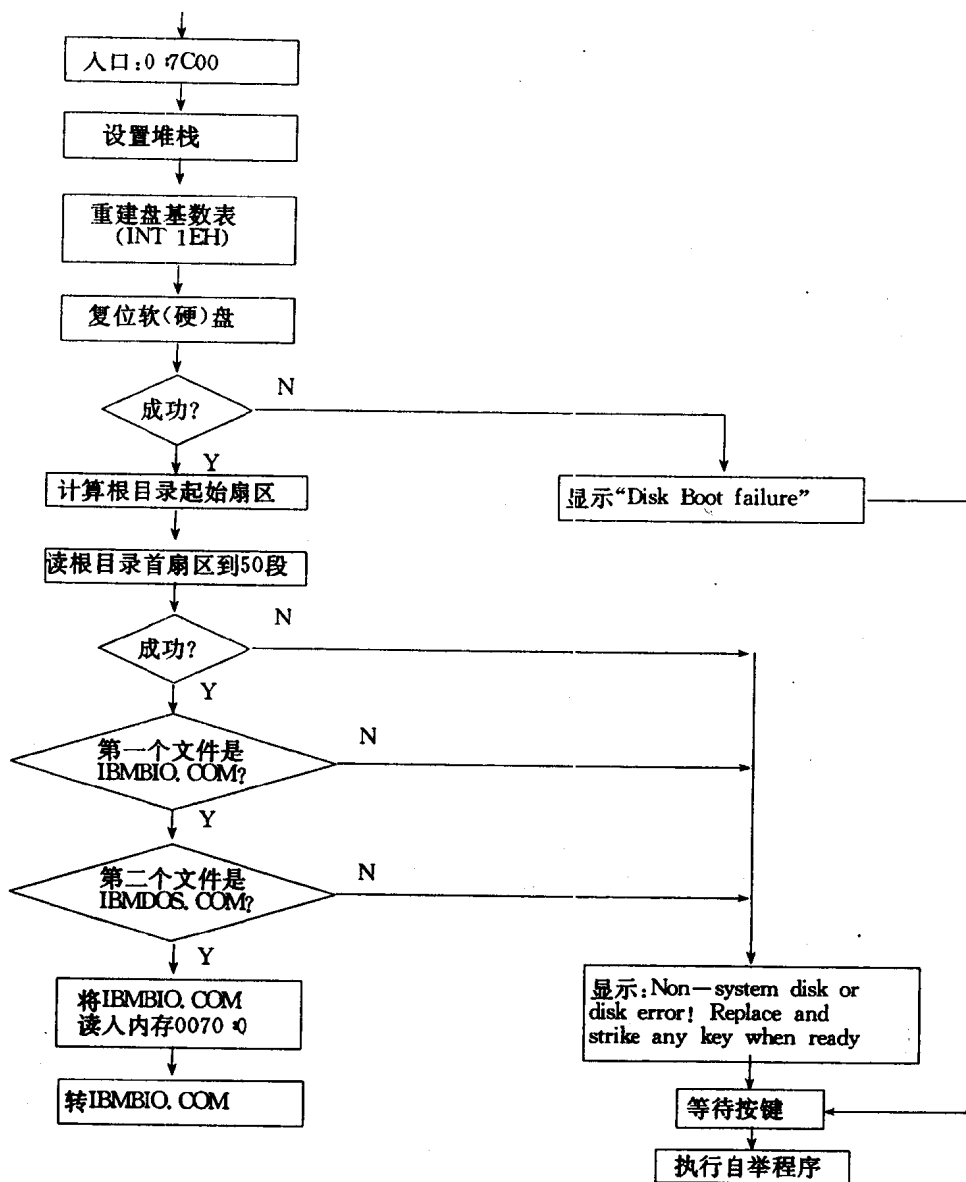


图 1.3.4 BOOT 程序流程图

在初始化过程中，以上地址完全被打乱，并伴有大规模的程序移动。具体的初始工作有如下几个方面：

(1) 在内存 50 段位移 70 处建立“磁盘基数表”。该表由 11 个字节组成，其内容反映了磁盘驱动器的工作参数，如：马达步进速率、磁头装载和卸载时间、每扇区字节数、每道扇区数，以及格式化扇区的间隔字节和填充字节等。这些参数是磁盘驱动器正常运行所不可缺少的。该基数表原来固化在 ROM—BIOS 的位移 F000: FEC7 处，现将其移至 50: 70 处，故必须重新设置向量 1EH 的入口。向量 1EH 是 ROM—BIOS 规定用于存放磁盘基数表地址的，并由 INT13H 所调用。

(2) 中断向量 1、3 和 4 是内中断，分别表示单步、断点和溢出中断。中断向量 1BH 用于处理 CTRL—BREAK 键盘中止键。这些向量指示的原中断例程均无实质性的处理程序。现在由初始化程序为其设置新的向量入口，用于指向由 DOS 提供的中断例程。

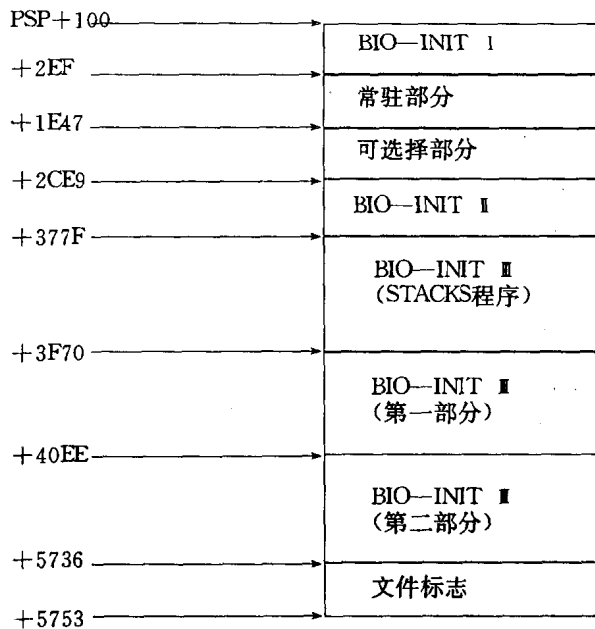


图 1.3.5 静态 IBMBIO.COM 文件构成

- (3) 通过调用ROM—BIOS 的 INT11H 和 INT12H 来确定系统硬件的配置和 RAM 的实际容量，供以后 DOS 管理系统设备和内存空间时使用。
 - (4) 初始化打印机口、异步通讯口和实时钟设备。
 - (5) 为系统配置的软驱、硬盘机及硬盘上的非本原驱动器依次创建块设备参数表 BPT。
 - (6) 将 BIO—INIT III 移到内存高端并将 IBMDOS.COM 读入内存预定位置。
- 以上这些工作由 BIO—INIT I 和 BIO—INIT II 来完成，具体工作流程如图 1.3.6。

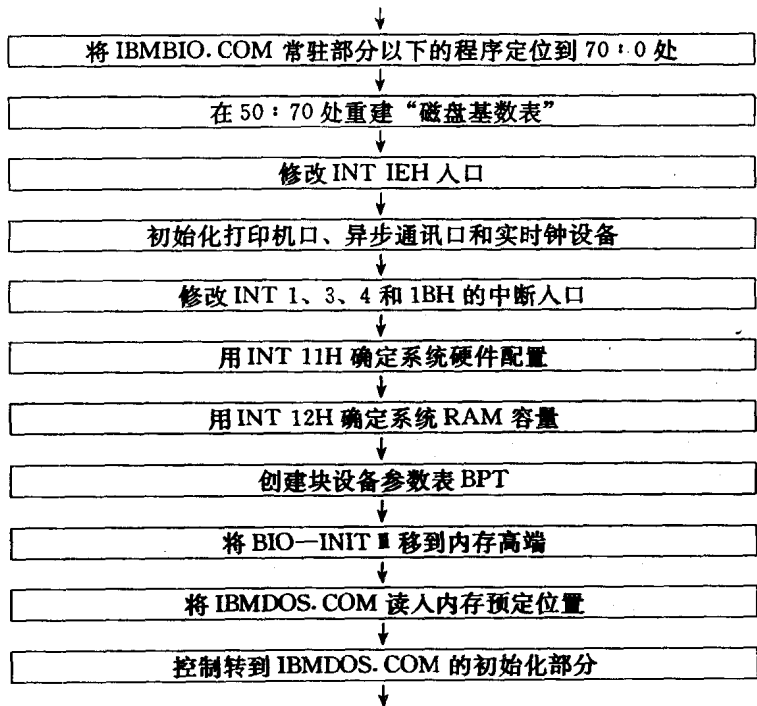


图 1.3.6 IBMBIO.COM 初始化流程图

5. IBMDOS.COM 初始化

IBMDOS.COM 的初始化是由 BIO—INIT Ⅲ 协同 IBMDOS.COM 的初始化部分来完成的。具体的初始化工作分为两个阶段：

第一阶段：由 BIO—INIT Ⅲ 的第一部分远调用 IBMDOS.COM 的初始化部分，完成后，远返回到 BIO—INIT Ⅲ 的第二部分。

这个阶段完成的具体工作是：

(1) 在初始化 DOS 内核模块需用的内部表和工作区之后，对 DOS 中断使用的 8 个向量入口进行预设置。由于中断 20H、21H、25H 和 26H 所对应的中断例程已随 IBMBIO.COM 和 IBMDOS.COM 的加载而常驻内存，故可以确定其最终位置，而另外 4 个中断向量 22H、23H、24H 和 27H 还须在 COMMAND.COM 加载后才能最终确定。

(2) 对常驻的设备驱动程序组成的设备链进行检查，并调用这些设备驱动程序的初始化功能。这些设备驱动程序的初始化工作主要是确定设备的状态，完成相应设备的初始化，同时为该设备驱动程序所管理的外部硬件中断建立中断向量。

对块设备驱动程序而言，初始化程序要关注该设备驱动程序所返回的磁盘参量，据此建立一张“磁盘 I/O 参数表”。该表内含 19 个字节，其内容包括：文件分配表个数、文件目录项数、起始扇区号、所占扇区数以及每簇扇区数等。这些参数是 DOS 进行文件管理的重要数据。

(3) 建立缺省的磁盘扇区缓冲区（2 个）和缺省的文件句柄控制块（8 个）。

第二阶段：由 BIO—INIT Ⅲ 的第二部分继续进行系统初始化工作。根据 CONFIG.SYS 文件完成系统配置，加载命令处理程序 COMMAND.COM。

这个阶段完成的具体工作是：

(1) 利用 DOS 系统功能调用 INT21H 的打开文件子功能 (3DH) 打开系统配置文件 CONFIG.SYS，并依次解释每一条命令，根据指定的配置命令建立 DOS 运行的系统环境。这些环境主要有：

按“BUFFERS=”命令开辟指定的磁盘扇区缓冲区；

按“FILES=”命令设置指定的同时打开的文件句柄控制块；

按“DEVICE=”命令加载指定的可安装设备驱动程序；

按“FCBS=”命令设置网络共享文件时可以同时打开的 FCB 数。

(2) 当可安装的设备驱动程序被依次加载时，调用相应的初始化功能以确定设备的状态并返回所占的内存容量，然后将其连接到设备链中。连接时将每一设备驱动程序中的设备头部“连接域”指向链中下一个设备驱动程序的段和偏移地址，如此依次连接，直至链中最后一个设备驱动程序的“连接域”为 -1，-1 为止。

(3) 处理完 CONFIG.SYS 文件后，关闭所有已打开的文件句柄，并为常驻的设备驱动程序 CON、AUX 和 PRN 分配头 5 个句柄号 (0—4)，将这些句柄提供给标准输入、标准输出、标准错误、标准辅助和标准列表设备，以便 DOS 或应用程序使用它们时不必再打开。

(4) 执行了系统配置文件 CONFIG.SYS 后，DOS 就能确定加载程序区的段首址并建立程序段前缀 PSP。此后，由 BIO—INIT Ⅲ 的第二部分加载命令处理程序 COMMAND.COM，并将其常驻部分 CCPR 安装在 PSP 之后，而将其暂驻部分 CCPT 安装在当前 RAM 的最高端。这样，在 CCPR 和 CCPT 之间的空间就是供用户使用的自由存储空间。

经过以上两个阶段的工作，BIO—INIT 完成了所有的初始化工作，随后即释放所占用的空间，将控制权交给 COMMAND.COM 去进行命令处理程序的初始化工作。

6. COMMAND.COM 初始化

IBMDOS.COM 的初始化工作完成后，控制权移交给 COMMAND.COM 的初始化程序。该程序主要完成以下的初始化工作：

(1) 对常驻中断例程 22H、23H、24H 和 27H 重新设置向量入口，供 DOS 系统使用。

(2) 检查自动执行的批处理文件 AUTOEXEC.BAT 是否存在。若存在该文件，则转至暂驻部分 CCPT，由其内部的批处理程序读入该文件并执行。在执行过程中，COMMAND.COM 的初始化程序被批命令处理程序所覆盖。所有批命令执行完毕后，由批处理程序返回到 COMMAND.COM 的常驻部分 CCPR，并显示 DOS 提示符 C>（或 A>）。

若 AUTOEXEC.BAT 文件不存在，则显示日期和时间提示，等待用户键入指定的日期和时间（或缺省选择）。系统记录下当前的日期和时间之后，显示 DOS 提示符 C>（或 A>），表明 DOS 启动成功，等待用户输入 DOS 命令。

至此，完成了整个的 DOS 引导过程，系统进入 DOS 开工状态。

COMMAND.COM 初始化过程的流程图如图 1.3.7。

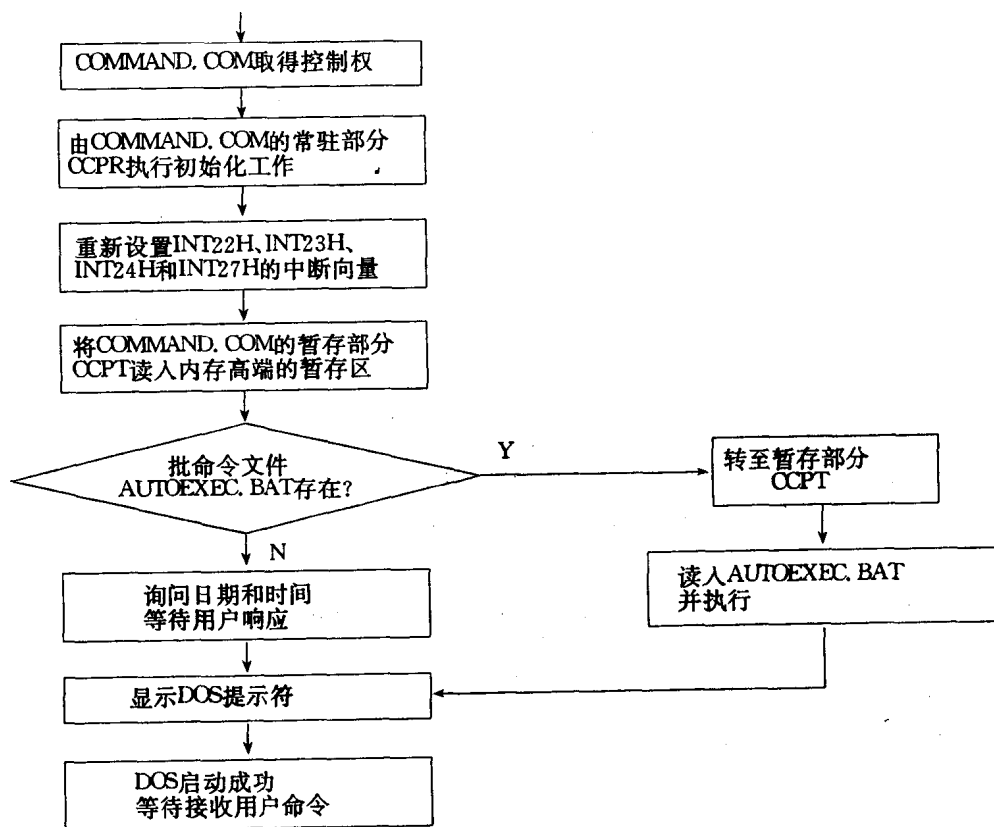


图 1.3.7 COMMAND.COM 初始化流程图