DOS 6.22

内核分析与内存管理技术

肖金秀 编著

中国大地出版社

责任编辑　王慧军
封面设计　凌　波

ISBN 7-80097-135-X

9 787800 971358 >

ISBN 7-80097-135-X/G·13
定价:28.00 元

DOS 6.22 内核分析与内存管理技术

肖金秀 编著

中 国 大 地 出 版 社

内容简介

本书主要分析 DOS 6.0 以上操作系统的内核结构及 DOS 内存管理技术。前者强调在 DOS 内核中用到的有关数据结构。以 DOS 系统链表为主干，详细地分析、深入地介绍、探讨各结构及它们之间的联系。涉及的结构有：MCB 内存控制块、SCPB 系统链指针块、SDA DOS 可交换数据区、CDS 当前目前结构、文件控制块 FCB、FAT 文件分配表、SFT 系统文件表、JFT 任务文件表、PSP 程序段前缀、DPB 驱动器参数表、磁盘 I/0 参数块 BPB 等。还包括了对.EXE 文件的加载过程及 EXEC 功能的调用。后者强调如何对 DOS 的内存进行优化和使用。

本书适应于计算机技术人员、大中院校学生及广大计算机爱好者，还可作为高等院校计算机应用专业，操作系统分析的典型教材。

图书在版编目（CIP）数据

DOS 6.22 内核分析与内存管理技术 / 肖金秀 编著. —北京：
中国大地出版社，1997.11
ISBN 7-80097-135-X

Ⅰ. D... Ⅱ. 肖... Ⅲ. 磁盘操作系统，DOS6.22 Ⅳ. TP361

中国版本图书馆 CIP 数据核字（97）第 24253 号

DOS 6.22 内核分析与内存管理技术

肖金秀 编 著

责任编辑：王慧军

特约编辑：张 青

中国大地出版社出版发行

（100081 北京海淀区大柳树路 21 号）

广东省农垦总局印刷厂

1998 年 1 月第 1 版 1998 年 1 月第 1 次印刷

开本：787×1092 毫米 1/16 印张：16 字数：369 千字

定价：**28.00** 元

编者的话

微型计算机的主流操作系统 MS-DOS，至今为止，已正式发表了十多个版本（DOS V1.0～DOS V6.22），以适应当代计算机硬件技术的迅速发展。没有人会怀疑 MS-DOS 的成功。据微软公司和工业分析家的报告，全世界已有 5 千万台计算机运行 MS-DOS，有 1 亿用户在使用 MS-DOS。这一巨大市场规模意味着，存在大量成功的应用软件在 DOS 上运行，使其生命力得以延续，十几年来久盛不变，深受用户欢迎。

当然，目前在个人计算机的领域里已经到处飞扬着 Windows95、Windows NT、Internet、Intranet 等新潮的字眼，MS-DOS 有被赶到角落里的趋势。坦率地说，谁也不会怀疑 MS-DOS 终被新的操作系统所取替，你也会成为 Windows 的用户，或是从 Windows 中运行 DOS。但是，任何技术生命的终结不可能骤然地发生。MS-DOS 仗着十多年来辉煌的发展历史、强大的应用软件开发商和庞大的用户群，靠丰富的应用软件的支撑及用户顽固的使用习惯，而没那么轻易地退出自己的阵地。说到这里，我想起了 LQ-1600K 的故事，EPSON 公司成功地开发了适合中国人使用习惯的 LQ-1600K 针式打印机，尽管公司在它的基础上开发了一系列新式的功能更强的针式打印机。但是，由于 LQ-1600K 操作简单，“透明”、“任打不烦”而使人们对它着魔，至今为止，LQ-1600K 还在针式打印机当中立于不败之地。这就是“先入主”和习惯性的可怕之处。

同样，DOS 用户已经完全驯服了 DOS 这匹白马，这匹白马的脾性已经对主人完全透明了，它是那么容易指挥、调教和打扮。而现在的那匹黑马 Windows95，带有一种傲气和霸气，使人们无法摸着它的脾气和性格，被它的一句话“你们不用管了，我们都已经做好了”而镇住了。变成不是你驾驭它，而是它牵着你走。天才的计算机专家和狂热的计算机玩家里最不服气它傲慢的态度。这可能是 DOS 的透明度，使人们较容易地了解和掌握 DOS 的全部功能，甚至可以进入 DOS 的内核，去了解 DOS 的数据结构。同时更由于 DOS 灵活性和可开发性，软件开发者能够迫使 DOS 按他们的意思行事，根据不同的需要，开发出高质量的应用程序和系统程序。

另外，Microsoft 公司声称，Windows95 在向下兼容性上做了巨大的努力，这只是主观上的意愿，客观上是难以做到百分之百的兼容。常玩游戏的人对此的认识颇有深度。因此，众多在 DOS 基础上开发的用户，要转入 Windows，那是一件谈何容易的事，除了习惯性作怪外，还有巨大的修改转换的资金在作梗。常言道：兵马未动，粮草先行嘛！

其次，Windows95 仍然依赖于 DOS 系统，它是建立在 DOS 基础上的完整的操作系统，DOS 仍然是 Windows95 的基础。安装了 Windows95 的计算机实际上装载了 DOS 的一个修改版本，它为 DOS7.0，它随 Windows95 一起自动安装到你的 PC 机上，并负责引

此为试读，需要完整PDF请访问：www.ertongbook.com

导你的 PC 机。可以说，学习和分析 DOS 内核后，你也许会去分析 Windows95，为今后的分析打下良好的基础，其次，对计算机病毒的防治、分析、清除均大有帮助。

本人在暨南大学计算机科学系讲授《DOS 6.22 内核分析与内存管理技术》课程多年，本课程专为本科高年级学生开设。因为它的技术性、先进性，以及实践性而深受学生的欢迎。

综上所述，我相信已经是要出版本书的最好理由了。

本书是在原讲义的基础上进行修改、补充而成。

本书的特点：

第三章：它介绍 DOS 内核中三个堆栈使用规则、Indos 标志、DOS 不可重入，应用程序中怎样解决 DOS 重入问题，提供如何避免重入的几种方法。

第五章：介绍如何对 DOS 内存进行优化。

第六章：对.EXE 文件的文件头进行较详细分析，用一例子说明一个.EXE 文件加载到内存的重定位全过程 ，达到全面了解.EXE 文件的全貌。

第七章：进程管理，介绍 PSP 程序段前缀，它是进程管理的关键数据结构，在本书中作为 DOS 的核心结构重点介绍，与该结构有联系的有：MCB、EVB、FDT、SFT、FCB 结构。其次还有很多概念均与 PSP 有关。如进入 DOS 内核的几种方法，子进程如何继承父进程打开的文件句柄等。

第八章：介绍 EXEC4BH 功能几种加载方法。应用程序中如何使用 EXEC 功能去加载一个子进程到内存并执行。

第九章：以 SFT 结构作为文件的主流去介绍 DOS 文件系统。

第十二章：如何编写 TSR 程序，以一些实例来说明要考虑的问题。

暨南大学计算机科学系软件专业 94 级的赖泽武参与本书第五章内容的整理和补充，廖疆星、陈霄峰参与本书十二章的整理和补充， 廖疆星，陈霄峰，罗云梅参与了本书实例的整理。在此表示衷心的感谢。

在讲课期间及编写本书时，也参考了大量有关的书籍，另张青同志参与了本书编辑、编审工作，在此致以诚挚的感谢。也在此对这些书籍的作者致以诚挚的感谢。

本人已经竭尽全力编写本书，出于各种原因，当中难免有不少错误和不足之处，恳请广大读者批评指正。

编 者

1997/11/26

目　录

目　录

目　录

目　录

第一章　DOS 磁盘数据结构及硬盘分区

1.1　DOS 磁盘数据结构

磁盘是一种外部存储设备，它用于长期保存数据及信息。通常采用的磁盘分软盘、硬盘两大类。对任何不同介质的磁盘都存在两种格式：物理格式和逻辑格式。磁盘物理格式决定了一个磁盘的面数（磁头数）、每面磁道数（柱面数）、每磁道扇区数（柱面）和每扇区字节数，而磁盘逻辑格式决定了 DOS 对磁盘信息的组织机制（软盘和硬盘有所区别）。

1.1.1　软盘的物理格式与逻辑格式

磁盘的物理格式对不同类型的软盘和硬盘都是一样的，FORMAT 命令对软盘主要完成两项操作：

- 物理格式化（低级格式化）
- 逻辑格式化（高级格式化）

1. 物理格式化的作用：

将每个磁盘划分为若干个同心圆记录信息的磁道，每个磁道上又分成若干个扇区，每个扇区分成为地址区和数据区，其中地址区是供磁盘驱动器检索每个扇区的数据区而设置的相关地址信息，数据区即通常所说的每扇区字节数，是磁盘扇区与 RAM 真正交换的有用数据。

表 1-1 列出了各种 DOS 版本下所支持的磁盘物理格式。

表 1-1 DOS 磁盘物理格式

物理格式	磁面数	磁道数	扇区数	字节数	容量(B)	DOS 版本
D-9(双面 9 扇区)	2	40	9	512	360K	2.0+
QD-9(高密 9 扇区)	2	80	9	512	720K	3.2+
QD-15(高密 15 扇区)	2	80	15	512	1.2M	3.0+
QD-18(高密 18 扇区)	2	80	18	512	1.44M	3.3+
硬盘 2G	32	2080	63	512	2G	6.22

此为试读，需要完整PDF请访问：www.ertongbook.com

磁盘物理格式经 DOS 格式化后的磁盘容量计算公式如下：

格式化容量＝磁面数×磁道数×扇区数×512(字节)

2. 逻辑格式化的作用:

软盘的逻辑格式是由 FORMAT 命令建立的。它主要在软盘上建立四部分内容:

- DOS 引导记录
- 文件分配表 FAT
- 文件目录表 FDT
- 文件数据区 DATA

其结构如图 1-1 所示:

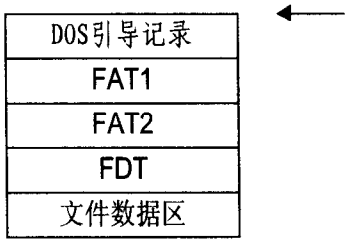


图 1-1　软盘逻辑结构

1.1.2　硬盘的物理格式与逻辑格式

硬盘用于 DOS 存取文件之前，必须经过如下三个步骤:

- 低级格式化（物理格式化）；
- 使用 FDISK 命令进行分区；
- 使用 FORMAT 命令进行高级格式化；

低级格式化的作用：

给硬盘划分成若干个柱面及每柱的扇区数和磁头数（硬盘在出厂之前已完成了物理格式化，即标明硬盘类型），并在每个扇区上记录相应的地址信息。在有的硬盘驱动器外壳盖上，对存在损坏的扇区，还贴有缺陷表，指出坏扇区的具体物理位置。

1.1.3 硬盘的逻辑格式

硬盘的逻辑格式也是通过 FORMAT 命令来建立的。对硬盘来说，由于它可以允许多

种操作系统来共享硬盘，因此，它必须在物理格式化后先使用分区命令 FDISK，建立 DOS 分区； 然后才能使用 FORMAT 命令建立 DOS 硬盘逻辑格式。其结构如图 1-2 所示：

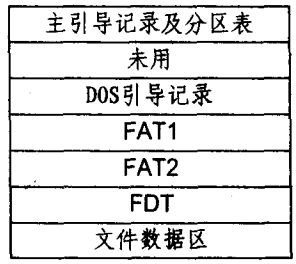


图 1-2　硬盘逻辑结构

下面的图 1-3 描述了软盘或硬盘 DOS 分区经 FORMAT 命令后被逻辑划分为引导扇区(BOOT)、文件分配表区(FAT)、根目录区(FDT)和文件数据区(DATA)以及占用的扇区数。此处 DOS 使用的是逻辑扇区，其编号是以 0 开始的逐柱、 逐头统一编号，被称为扇区的逻辑地址，简称为逻辑扇区号(相对扇区号)

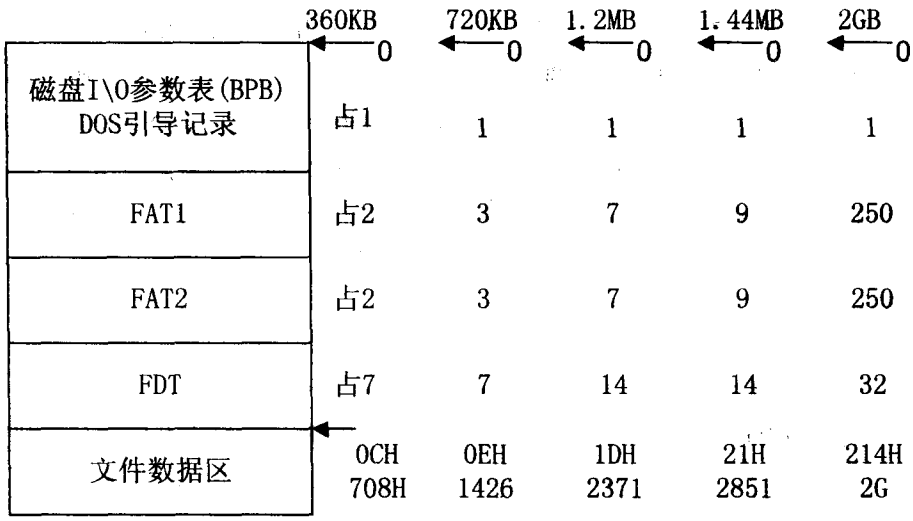


图 1-3　磁盘逻辑格式布局及各部分扇区数

1.1.4 逻辑扇区与物理扇区的关系

磁盘经 FORMAT 格式化后，在 DOS 这个层次上对磁盘的操作均采用逻辑扇区为访问对象。它对磁头、磁道、扇区数据序列的简化是给每一扇区赋予唯一的逻辑扇区号。第一磁头的第一磁道的第一扇区(H=0，T=00，S=1)，变成逻辑扇区号(LSN)000，同一磁表面同一磁道的其余扇区分别依次排序，然后 LSN 跳到磁盘的其它面。

相对编号的顺序是，对某一磁道，先编最低号磁头下的所有扇区号，然后编下一磁头号下的所有扇区号，直到该磁道所有磁头号下的所有扇区都编完，再进到下一个磁道，依次类推，最后编到最高号磁道上最高号磁头下的最后一个扇区为止。简言之，先变扇区，然后变磁头，最后变磁道。对于 360KB 的软盘，0 面 0 磁道上的第 1-9 扇区，分别对应 LSN 的 000-008，LSN 为 009 表示的是指 1 面 0 磁道下的第 1 扇区(H=1，T=00，S=1)。而(H=0，T=01，S=1)则为 LSN 018。

所谓物理扇区是指绝对位置上的扇区，它有三个相关参数：磁道号(C)， 磁头号(H)和扇区号(S)。前二者从 0 开始编号，最后者是从 1 开始编号。

对其它不同容量的磁盘，上述的转换可能不同，但从磁头、磁道、扇区转化成唯一的 LSN 的原则是一致的。基于此，由 DOS 操作使用的逻辑扇区号转换成物理磁道号、 物理磁头号和物理扇区号是通过 DOS 设备驱动层(DOS_BIOS)的块设备驱动程序来完成的。

1.2 硬盘分区及其应用

在 MS-DOS 操作系统中，一个硬盘可分成 4 个不同的分区， 以存放 4 种不同的操作系统，达到多种操作系统可共享硬盘空间的目的。 随着大容量硬盘的出现，利用 FDISK 命令还可将一个大容量硬盘划分为一个自举 DOS 分区和一个扩展 DOS 分区。扩展 DOS 分区可用于存放非系统文件，将扩展 DOS 分区作为逻辑驱动器被用户访问，最多定义为 23 个逻辑驱动器，其编号依次为 D、E、F...。它们如同实际驱动器一样使用。

1.2.1 硬盘分区

硬盘分区的目的:

DOS 当初的设计是支持多种操作系统共享硬盘空间， 以硬盘分区表结构描述各种操作系统占用的硬盘分区容量，将每个操作系统分别存放在各自的分区表内，每次只能指定任一个分区的操作系统为活动分区（启动状态）。其余的分区自动设置为非活动分区。

1.2.2 DOS 硬盘分区命令

从 DOS3.30 开始，使用 FDISK 命令可建立一个 DOS 扩展分区， 以支持大容量硬盘的要求。

FDISK 命令在不同 DOS 版本的区别:

DOS 3.3 版　　允许建立一个主 DOS 分区和一个扩展 DOS 分区。主 DOS 分区不能超过 32MB；扩展分区若超过 32MB，即必须将它进一

分成若干个不超过 32MB 的逻辑盘 E:～Z:。

DOS 4.0～6.2 版　允许硬盘上最多有 4 个分区，可有一个主 DOS 分区和一个扩展 DOS 分区，扩展 DOS 分区又可分成若干个逻辑盘，其大小可大于 32MB，不受限制（只要在硬盘容量允许的情况下）。

（4.0 版本开始，BPB 中“总扇区数”由原来的 1 字长改为 2 字长，DOS 分区的大小才突破了 32MB 的限制，现它可建立最大为 2GB 的磁盘分区。）

FDISK 命令采用菜单驱动方式，它的主菜单有如下选择项：

1） Create DOS Partition。

2） Change Active partition。

3） Delete DOS partition。

4） Display Partition Information。

5） Select Next Fixed Disk Drive。

最后一项适用于多个硬盘系统。

通常，DOS 分区是以柱面为分配单位，分区容量即取决于所占用的柱面数。因此，实际分区的容量是按下式确定：

分区容量＝磁头数×柱面数×每柱扇区数×每扇区字节数

不同类型的硬盘一般都选用每柱扇区数为 17，每扇区字节数为 512B，只是磁头数不尽相同。而 2GB 磁盘每柱扇区数为 63(3FH)，因此，用户应选用多少柱面数来确定合理的分区容量，应查阅该硬盘含有的磁头数。

一般使用 DOS6.22 版本的 FDISK 时，初始 DOS 分区总是从 0 柱 1 头 1 扇区开始，即前面留有 0 柱 0 头下的 63 个扇区作为隐含扇区。其中，第一个扇区保存硬盘主引导记录和分区表信息，供系统启动时使用，其它 62 个扇区保留未用。

注意：所谓隐含扇区是指 DOS 分区无法管理的区域。DOS 任何磁盘操作对它不起作用，除非采用 ROM_BIOS 的 INT 13H 才能访问到它。

1.2.3 硬盘分区表链

1. 分区表链结构

分区表链的布局结构如图 1-4 所示。

由图 1-4 可获知如下信息：

分区表链位于 0 柱 0 头 1 扇区内、以位移 1BEH 开始的第一分区表作为链首，由表内的链接表项指示下一分区表的物理位置（XX 柱 0 头 1 扇区），在该位置的扇区内同样位移 1BEH 处，保存着第二张分区表，依次类推，直至指向最后一张分区表的物理位置（YY

柱 0 头 1 扇区）。因该分区表内不存在链接表项，即作为分区表链的链尾。

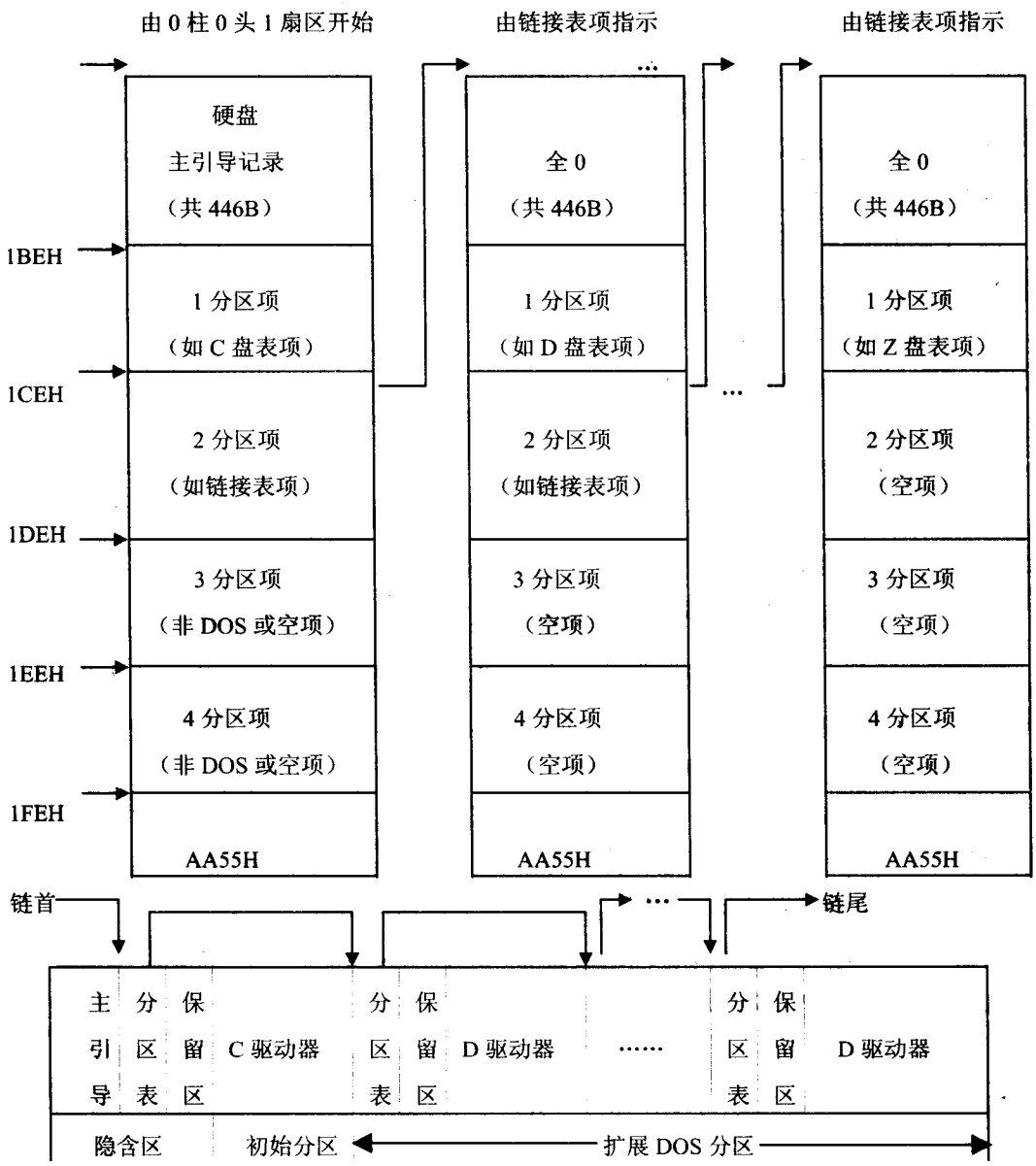


图 1-4 分区表链的布局结构示意

2. 分区表项定义

无论分区表项是什么类型，它总是占 16 个字节，其结构和定义如图 1-5 所示。

位移	0	1	2	3	4	5	6	7	8 9 10 11	12 13 14 15
	Bi	H	S	C	Si	H	S	C	相对扇区号	总 扇 区 数
	起始地址				终止地址					

图 1-5 分区表项的结构和定义示意

对于 DOS 环境下的分区表项，我们感兴趣的是 DOS 表项和链接表项两种，它们的结构布局是一样的，但具体的含义稍有差别。现分别列于表 1-2 中。硬盘主引导记录的结构和扩展 DOS 分区的主引导记录的结构如图 1-6、图 1-7 所示：

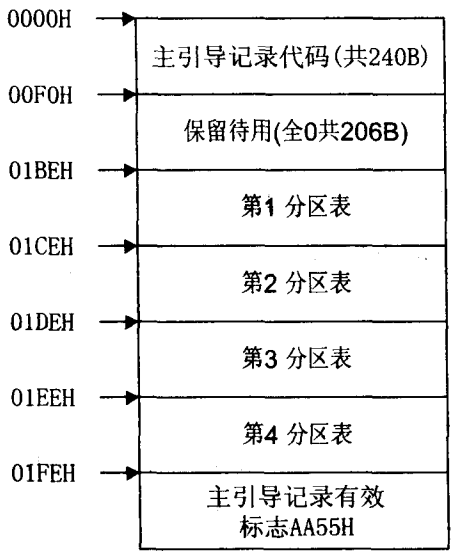


图 1-6 硬盘主引导记录的结构

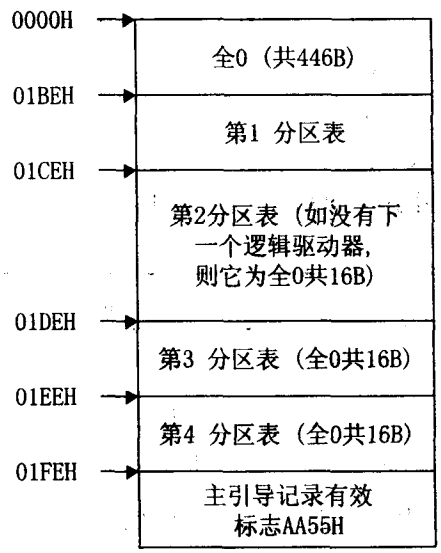
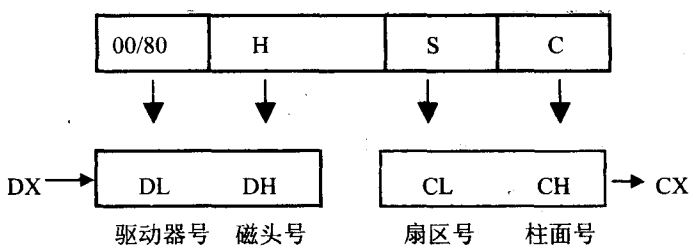


图 1-7 扩展 DOS 分区的主引导记录的结构

在分区表项中，它们的起始地址和终止地址由三个字节组成，其中，H 指磁头号、S 指扇区号（低 16 位），C 指柱面号（低 8 位）。柱面号的高 2 位存放在 S 字节的高 2 位里， 即柱面由 10 位组成。这 10 位的柱面号可表示 1023 柱(1GB)。在 INT 13h 磁盘 I/O 操作中，寄存器 DX 和 CX 与驱动器号、磁头号、扇区号和柱面号的关系如下所示：



此为试读，需要完整PDF请访问：www.ertongbook.com