2、引导扇区结构

硬盘分区表位于引导扇区内。主引导扇区（Boot Sector）也就是硬盘的第一个扇区， 它由主引导记录（MBR：Master Boot Record），主分区表（DPT：Disk Partition Table）和引导区标记（Boot Record ID）三部分组成。分区引导扇区位于每个分区的第一个扇区，由分区引导记录、分区链表、引导区标记三部分组成。下面介绍主引导扇区的结构，分区引导扇区的结构与此相同。

主引导记录占用引导扇区的前 446 字节(0 到 1BDH)，存放系统主引导程序，负责从活动分区中装载并运行系统引导程序。主分区表占用 64 字节(1BEH 到 1FDH)，记录了磁盘的基本分区信息。主分区表分为四个分区项，每项 16 字节，分别记录了每个主分区的信息。引导区标记占用两个字节 (1FEH 和 1FFH)，对于合法引导区，它等于 AA55H。

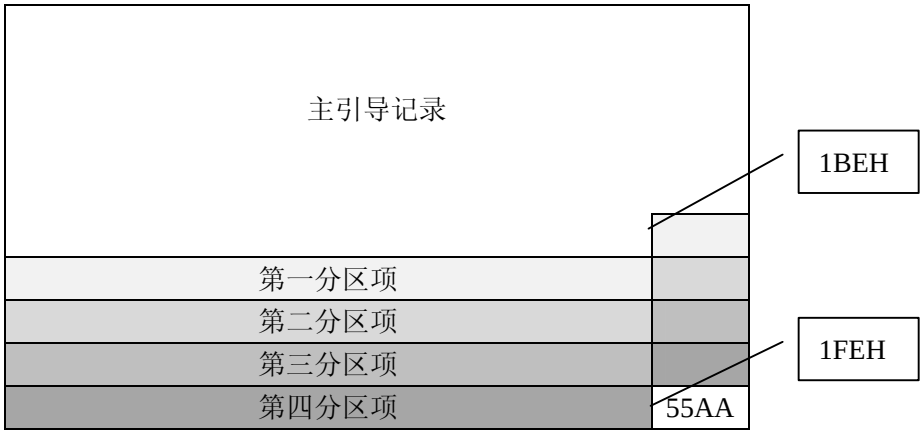

图 6.2　　主引导扇区结构

3、分区表结构

在主引导区中，从地址 1BEH 开始，到 1FDH 为止的 64 个字节中的内容是分区表，每个分区占用 16 个字节，因此一个硬盘最多只能分成四个主分区，其中扩展分区也是一个主分区。所谓扩展分区，严格地讲它不是一个实际意义的分区，它仅仅是一个指向下一个分区的指针，这种指针结构将形成一个单向链表。这样在主引导扇区中除了主分区外，仅需要存储一个被称为扩展分区的分区数据，通过这个扩展分区的数据可以找到下一个分区（实际上也就是下一个逻辑磁盘）的起始位置，以此起始位置类推可以找到所有的分区。无论系统中建立多少个逻辑磁盘，在主引导扇区中通过一个扩展分区的参数就可以逐个找到每一个逻辑磁

盘。

分区表的格式如表 6.1 所示。表中显示的偏移量是第一分区的值，下面各分区按照相同的规律递增[23][24][25]。

表 6.1　　分区表格式

项目	偏移量	数据类型	内容说明
1	1beH	BYTE	State：分区状态。80H 表示可启动分区，00H 表示不可启动
2	1bfH	BYTE	StartHead：分区起始磁头号
3	1c0H	WORD	StartSC：分区起始扇区值和柱面值
4	1c2H	BYTE	Type：分区类型。常用的字节标志有： 05H 或 0fH：表示扩展 MSDOS 分区； 06H 或 0eH：表示 FAT16；0bH 或 0cH：表示 FAT32。
5	1c3H	BYTE	EndHead：分区结束磁头号
6	1c4H	WORD	EndSC：分区结束扇区值和柱面值
7	1c6H	DWORD	Relative：分区前扇区数（相对值）
8	1caH	DWORD	Sectors：本分区扇区数（绝对值）

其中第 2、3 项和第 5、6 项适用于 CHS 模式，在硬盘的 8G 以下区域仍表示地址信息。但对于超过 8G 的区域，这几部分的数据已不具有参考价值；这时要参考的数值为第 7 项和第 8 项，其中第 7 项数据尤为重要。

由主分区表中的数据即可依次得到各分区的信息，并可对各分区数据进行操作，如恢复数据、隐藏分区、按分区加密等等。

6.2　实例介绍

一块硬盘共 30G，分成六个区，各分区大小分别为 C 盘：3G；D 盘：3.5G；E 盘：4.5G；F 盘：5G；G 盘：1G；H 盘：13G。

1、读 C 盘分区表

用扩展 int 13H 读出 0 扇区的分区表信息如下（具体操作见下节）：

80　01　01　00　0B　FE　7F　7E　|　3F　00　00　00　80　E2　5D　00

00　00　41　7F　0F　FE　FF　FF　|　BF　E2　5D　00　18　AF　35　03

第一分区项表示 C 盘的信息：起始扇区为第 7 项 0000003FH（63：十进制数），这个数值为扇区相对位置，其参考点为整个硬盘的 0 扇区；分区大小为第 8 项

005DE280H（6152832），这个数值不包括隐藏的 63 个扇区；因此结束扇区为 3FH＋5DE280H＝5DE2BFH（6152895）。第二分区项表示整个扩展分区的信息：起始扇区为第 7 项 005DE2BFH（6152895），这个数据也是一个相对数值，其参考点为整个硬盘的 0 扇区；扩展分区大小为 0335AF18H（53849880），对于本例就是其他 DEFGH 五个分区的扇区总数。

再明确一下，D 盘起始扇区：005DE2BFH（6152895）。

2、读 D 盘分区表

根据第 1 步得到的数值，，用扩展 int 13H 读出 D 盘起始扇区的分区表信息：

00　01　41　7F　0B　FE　FF　03　|　3F　00　00　00　06　5B　5F　00

00　00　C1　04　05　FE　7F　41　|　45　5B　5F　00 BE　B4　8C　00

其中第一分区项表示 D 盘的信息：起始扇区为 0000003FH（63：十进制数），这个数值为扇区相对位置，其参考点为扩展分区的 0 扇区，即 005DE2BFH（6152895）；分区大小为 005F5B06H，不包括隐藏的 63 个扇区。第二分区项表示下一分区，即 E 盘的信息：起始扇区为带下划线的数值 005F5B45H（6249285），这个数据也是一个相对数值，其参考点为扩展分区的 0 扇区，即 D 盘的起始扇区 005DE2BFH（6152895），则 E 盘的起始扇区为 5DE2BFH＋5F5B45H＝BD3E04H（12402180），这个数值也可以由 D 盘的绝对起始扇区加上 D 盘的绝对大小得到，即 5DE2BFH+5F5B06H+3FH=BD3E04H；E 盘大小为 008CB4BEH（9221310），这个是包含隐藏扇区在内的绝对大小。

E 盘起始扇区：00BD3E04H（12402180）。

3、读 E 盘分区表

根据第 2 步计算出来的数值，用扩展 int 13H 读出 E 盘起始扇区的分区表信息：

00　01　C1　04　0B　FE　7F　41　|　3F　00　00　00　7F　B4　8C　00

00　00　41　42　05　FE　FF　BF　|　03　10　EC　00　FE　64　9C　00

分析该扇区的数据：第一分区项最后四字节 008CB47FH 是 E 盘大小，加上 3FH 后就是 E 盘绝对大小，和 D 盘分区表项的最后四字节 008CB4BEH 一致；F 盘的开始扇区为带下划线的数值与扩展分区的起始扇区之和，即

00EC1003H+005DE2BFH=0149F2C2H（21623490），或者由 E 盘的绝对大小加上 E 盘的起始扇区也可以得到，即 008CB4BEH+00BD3E04H=0149F2C2H。

4、读 F 盘分区表

用上述方法，可以读出 F 盘的分区表信息：

00　01　41　42　0B　FE　FF　BF　｜　3F　00　00　00　BF　64　9C　00

00　00　C1　C0　05　FE　3F　3F　|　01　75　88　01　80　60　1F　00

F 盘分区表数据分析与 E 盘一样，可算出 G 盘起始扇区为：01887501H+005DE2BFH=01E657C0H（31872960），或者由 009C64FEH+0149F2C2H=01E657C0H 也可以得到。

5、读 G 盘分区表

读出 F 盘的分区表信息：

00　01　C1　C0　0B　FE　3F　3F　|　3F　00　00　00　41　60　1F　00

00　00　01　40　05　FE　BF　96　|　81　D5　A7　01　97　D9　8D　01

可算出 H 盘起始扇区为：01A7D581H+005DE2BFH=0205B840H（33929280）。

6、读 H 盘分区表

读出 H 盘的分区表信息：

00　01　01　40　0B　FE　BF　96　|　3F　00　00　00　58　D9　8D　01

00　00　00　00　00　00　00　00　|　00　00　00　00　00　00　00　00

第二分区项数值全为 0，说明已没有下一分区，H 盘即为最后一个分区。最后一个分区的结束地址不能取下一分区的起始地址（此时为 0），而应取本分区的第八项，即分区大小，与本分区的起始地址求和，再加上隐藏的 63 个扇区，其结束扇区为：018DD958H+0205B840H+0000003FH=39391D7H（60002775）。把 D、E、F、G、H 五个分区的绝对大小加起来，3FH+5F5B06H+8CB4BEH+9C64FEH+1F6080H+18DD958H+3F=335AF18H，此即 C 盘分区表最后四字节的内容。

6.3　实际操作

读扇区要用到扩展 13H 中断，这里简要介绍一下，详细情况请参考有关资料。

1、扩展 int 13H