硬盘分区表与 BPB 表的关系及其应用

www.fpgadig.org

摘要 介绍了硬盘分区表与 BPB 表的参数间的关系，讨论了当其中的一个表受到损坏时，通过另一个表来恢复受损表的方法。

关键词 硬盘 分区表 BPB 恢复

硬盘分区表和 BPB 表是硬盘两个重要的数据区，这两个表如受到破坏，就会使硬盘不能正常工作。在实际中，由于病毒的入侵或人为的误操作，常会损坏这两个表中的某一个。这两个表所记录的信息有许多相似之处，因此，可以通过幸存的一个表来推出另一个表的信息。本文介绍这两个表之间的互推关系，并讨论在某一个表损坏时，通过另一个表修复受损表的方法。

1 硬盘分区表与 BPB 表的关系

1.1 硬盘分区表和扩展卷分区表[1]

硬盘分区表位于硬盘第一个扇区的偏移 01BEH 至 01FDH 间，记录各个分区的起止地址。它共有 4 个表项，每个表项 16 个字节，记录一个分区的起止地址，其具体内容见表 1。

表 1 硬盘分区表各项含义

内容		字节数
自举标志 BM		1
起始地址	起始磁头号 SH	1
	起始扇区号 SS	1
	起始柱面号 SC	1
系统标志 SM		1
终止地址	终止磁头号 EH	1
	终止扇区号 ES	1
	终止柱面号 EC	1
相对扇区号 RS		4
分区所用扇区数 TS		4

表 2 BPB 表各项含义

含义	字节数
每扇区字节数 BPS	2
每簇扇区数 SPC	1
保留扇区数 CS	2
FAT 表个数 FN	1
根目录登记项数 ND	2
磁盘总扇区数 TS0	2
磁盘介质描述符 DM	1
每个 FAT 的扇区数 SPF	2
每道扇区数 SPT	2
磁头数 HN	2
隐含扇区数 HS	4
磁盘上的总扇区数 TS1	4

在表 1 中，自举标志 BM 也称为活动分区指示符。对于活动分区，该标志为 80H，而对于非活动分区，该标志为 0。一般情况下，C 盘即第一个逻驱为活动分区，其它分区为非活动分区。

系统标志 SM 指明分区的操作系统类型，01 表示该分区采用 12 位 FAT，04 和 06 表示采用 16 位 FAT，05 表示该分区为 DOS 扩展分区。

相对扇区号 RS 及分区所用扇区数 TS 可以根据分区的起止地址计算出，因此，只要知道每个分区的起止地址，就可以确定分区表的各个参数。

扩充卷分区表记录 DOS 扩展分区各个扩充卷[①]的起止地址，它位于每个扩充卷第一个扇区的偏移 01BEH 至 01FDH 间，记录的内容与硬盘分区表的内容相似。

1.2 磁盘 BPB 表

磁盘 BPB 表位于磁盘 DOS 引导扇区的偏移地址 0BH~1DH 处，共 25 个字节。其具体内容见表 2。

在表 2 中，TS0 和 TS1 的含义是一样的，均指该磁盘所占的总扇区数。当总扇区数小于 10000H 时，用 TS0 表示，而 TS1 等于零；当总扇区数大于或等于 10000H

表 3 每簇扇区数与硬盘容量的关系

硬盘容量	每簇扇区数
0~16M	08
16~160M	04
160~256M	08
256M~	16

① DOS 扩充分区一般可分为多个扩充卷，每个扩充卷均由扩充主引导记录和逻辑驱动器组成。扩充主引导记录与主引导记录的结构相似，里面含有扩充卷分区表。

时，用 TS1 表示，而 TS0 等于零。

一般地，对硬盘而言，每扇区字节数 BPS 和根目录登记项数 DN 均为 512，保留扇区数 CS 为 1，FAT 个数 FN 为 2，磁盘介质描述标志 MD 为 F8H。

每簇扇区数 SPC 和每个 FAT 的扇区数 SPF 均与磁盘的容量即总扇区数有关。每簇扇区数与硬盘容量的关系见表 3，每个 FAT 的扇区数 SPF 可以根据每簇扇区数 SPC 及硬盘总扇区数 TS1 按下式计算出来：

SPF=ceil[(TS1-1)/SPC*(a/512)] （1）

式中，a 为与 FAT 位数有关的系数，对于 12 位 FAT，a 等于 1.5，对于 16 位 FAT，a 等于 2；

ceil 函数表示对计算出的实数值取不小于它的最小整数；

其它符号同表 1 和表 2。

1.3 硬盘分区表与 BPB 表相应参数间的关系

在上述两个表中，有一些参数是相同的，可以相互推出。主要包括：

(1)硬盘分区表中的相对扇区号 RS 与 BPB 表中的隐含扇区数 HS 相同；

(2)硬盘分区表中的分区所用扇区数 TS 与 BPB 表中的磁盘总扇区数 TS0 或 TS1 相同。

(3)一般情况下，硬盘分区表中的终止磁头号 EH 加 1 即为 BPB 表中的磁头数 HM，终止扇区号即为 BPB 表中的每道扇区数 SPT。

2 应用

2.1 由 BPB 表修复硬盘分区表

当硬盘分区表被破坏后，可以通过各逻辑驱动器的 BPB 表推出各分区的起止地址，从而恢复硬盘分区表和扩充卷分区表的内容。

硬盘分区表被破坏后，进入不了硬盘，须通过 BIOS 中断 INT 13H 才能读出 BPB 表的信息。BPB 表位于 DOS 引导记录内，一般说来，主 DOS 分区的 DOS 引导记录位于 0 柱面、1 号磁头的第一个扇区上，扩充卷的 DOS 引导记录位于扩充卷主引导记录的同一柱面的下一个磁头的第 1 扇区。

对于只有一个 DOS 主分区的硬盘，其分区表的恢复比较简单。首先，用 INT 13H 读出 0 柱面 1 磁头 1 扇区上的主分区 DOS 引导记录，得到 BPB 表；然后，根据 BPB 表确定主分区的起止地址，从而恢复分区表。一般情况下，主分区的起始柱面号 SC 为 0，起始磁头号 SH 均为 1，起始扇区号 SS 为 1。终止磁头号 EH 等于磁头数 HN 减 1，终止扇区号 ES 等于每道扇区数 SPT，终止柱面号 EC 可以根据 BPB 表中总扇区数 TS0(或 TS1)按下式计算出：

EC=[(TS1-ES)/SPT+SH-EH]/HN+SC （2）

式中各符号的意义见表 1 和表 2。

分区表中的相对扇区号 RS 和分区所用扇区数 TS 可以分别由 BPB 表中的隐含扇区数 HS 和磁盘总扇区数 TS0 或 TS1 得出。

对于含有 DOS 扩充分区的硬盘，首先要确定主分区的起止地址（方法同前），然后确定各个扩充卷的位置。对于扩充卷，其起止扇区号与主分区的一样，起始柱面号等于前一扩充卷（或主分区）的终止柱面号加 1，而其终止柱面号可按式(2)求出。

下面举例说明。

某硬盘分区表被破坏后，用 INT 13H 读出 0 柱面 0 磁头 1 扇区上的主分区 DOS 引导记录，得知其 BPB 表内容如下（均为 16 进制数）：

00 02 10 01 00 02 00 02 00 00 F8 FA 00 3F 00 40 00 3F 00 00 00 41 A0 0F 00

从表中可知，该硬盘的磁头数 HN 为 40H，每道扇区数 SPT 为 3FH，主分区的隐含扇区数 HS 为 3FH，总扇区数 TS1 为 FA041H。由此可推知，主分区的终止磁头号 EH 和终止扇区号 ES 均

为 3FH。由式（2）可求出主分区的终止柱面号 EC 为：

EC=0+[(FA041H-3FH)/3FH+1-3FH]/40H=FDH

因此，可知下一个扩充卷的 DOS 引导记录位于 FEH 柱面 1 磁头 1 扇区。读出该引导记录后，得知该逻辑驱动器 D 的 BPB 表内容如下：

00 02 20 01 00 02 00 02 00 00 F8 85 00 3F 00 40 00 3F 00 00 00 41 9C 10 00

由上表可知，该逻驱的总扇区数为 109C41H, 因此，其终止柱面号为：

EC=FEH+[(109C41H-3FH)/3FH+1-3FH]/40H=20BH

从 BIOS 参数可知，20BH 柱面为硬盘的最后一个柱面，因此，本硬盘只有两个逻驱：C 和 D。

从前面的分析，可知各个逻驱的起止地址（不包括主引导记录和扩充卷引导记录）如表 4 所示。

表 4 各个逻驱的起止地址

	起始磁头 SH	起始柱面 SC	起始扇区 SS	终止磁头 EH	终止柱面 EC	终止扇区 ES
C	1	0	1	3FH	FDH	3FH
D	1	FEH	1	3FH	20BH	3FH

根据上表就可以确定分区表和扩充卷分区表，这里不详细讨论。

2.2 由硬盘分区表修复 BPB 表

当 BPB 表被破坏后，可由硬盘分区表或扩充卷分区表中的各个表项确定各个扩充卷的 BPB 表。

隐含扇区数 HS 和磁盘上的总扇区数 TS0 或 TS1 可分别由硬盘分区表或扩充卷分区表中的相对扇区号 RS 和分区所用扇区数 TS 确定。

磁头数 HM 和每道扇区数 SPT 可分别由分区表中的终止磁头号 EH 和终止扇区号确定，也可以通过 BIOS 参数得出。

每扇区字节数 BPS、保留扇区数 CS、FAT 表个数 FN、根目录登记项数 DN 和磁盘介质描述符 MD 一般为常数，其数值详见 1.2 节。

每簇扇区数 SPC 可由表 3 确定出。

每个 FAT 的扇区数 SPF 可以由总扇区数 ST 按式（1）算出，也可用下面的方法来求。

一般地，每一个 DOS 分区均有两个 FAT，这两个 FAT 紧挨在一起。根据这个特点，可以由这两个 FAT 的起始位置确定出每个 FAT 的扇区数，也就是说，这两个 FAT 间的扇区数即为每个 FAT 所占的扇区数。

第一个 FAT 的起始位置比较容易确定，它一般位于 DOS 引导扇区之后。第二个 FAT 的位置需要根据其特征来确定。对硬盘而言，每个 FAT 的前四个字节均为“F8 FF FF FF”，因此，在第一个 FAT 之后且具有上述特征的扇区即为第二个 FAT 的起始地址。

3 结论

(1)硬盘分区表及磁盘 BPB 表的参数间可以相互推算出来，因此，当其中的某一个表被破坏后，可以通过另一个表恢复。

(2)本文所讨论的问题仅局限在硬盘仅使用 DOS 操作系统的情况，对于同时使用其它操作系统的硬盘，本文的结论不一定成立。

参考文献

1.贾建章，武万龙.硬盘逻驱加密技术.微型机与应用，1996.1

2.黄焕如.在硬盘上设置非 DOS 扇区.计算机工程,1993.2