第28卷第2期 上海师范大学学报(自然科学版) Vol. 28, No. 2
1999年6月 J. of Shanghai Teachers Univ. (Natural Sciences) Jun. 1999

硬盘主引导记录的数据重建

忻根勇

提　要　从硬盘主引导记录和分区表的结构着手, 介绍了硬盘主引导记录的查看及修改方法. 着重论述了如何在不破坏硬盘原有数据的情况下, 重建主引导记录的原理和方法.

关键词　主引导记录; 分区表结构; 中断向量; 驻留程序
中图法分类号　TP333.35

0　引　言

PC机在DOS下(包括WINDOWS)要使用硬盘, 首先需用FDISK.COM命令对其进行分区, 也就是创建硬盘主引导记录, 它对于硬盘意义重大. 如果硬盘主引导记录遭到破坏(主要是由病毒感染、误操作或硬盘磁介质受损等情况引起), 则将使硬盘无法正常使用. 目前硬盘已成为人们存贮数据信息最主要的器件, 若主引导记录遭到破坏, 将会给用户带来极其严重的损失. 研究主引导记录的意义就在于分析和理解它的结构, 从而能迅速、安全、有效地修正或重建被破坏的硬盘主引导记录.

1　主引导记录的结构

一个完整的硬盘主引导记录共有512个字节, 分为3个部分: 主引导记录程序区、硬盘分区表和硬盘赋权标记. 它们在硬盘中占用一个扇区, 该扇区位于硬盘的0面0道1扇区. 主引导记录的数据格式如下所示:

000	主引导程序(226个字节)						
	全零(220个字节)	0～3	BOOT	H	S	CYC	
1BE	第一分区表(16个字节)		标志	分区起始位置			
	第二分区表(16个字节)	4～7	SYS	H	S	CYC	
	第三分区表(16个字节)		标志	分区终止位置			
	第四分区表(16个字节)	8～B	相对扇区				
1FD	硬盘赋权标志55AA	C～F	实际总扇区数				

收稿日期: 1998-12-07

作者忻根勇, 男, 工程师, 上海师范大学实验室管理处, 上海, 200234

主引导程序区占用前 446 个字节, 实际使用 226 个字节左右, 其余为全零, 主要是为兼顾到其他操作系统或多个操作系统共存而保留扩展余地. 从 1BEH～1FDH 共 64 个字节为硬盘分区表, 可建 4 个分区表, 每个分区表占用 16 个字节, 记录着分区的信息, 最后 2 个字节存是硬盘赋权记录 55AA.

2 分区表结构

每个分区表 16 个字节意义如下:

字节	名称	表示值
0	自举标志 BOOT	00= 不可自举, 80= 可自举 (仅第一个分区即DOS 主分区才允许)
1～3	分区起始位置 H. S. C	分区在硬盘上始地址(磁头、扇区、柱面)
4	系统标志 SYS	00= 未定义, 01= DOS 分区 12 位 FAT, 02= UNIX 分区,
		04= DOS 分区 16 位 FAT, 05= 扩展DOS 分区, 06= DOS3. 3 以上
5～7	分区终止位置 H. S. C	分区在硬盘上终止地址(磁头、扇区、柱面)
8～B	相对扇区	以当前分区为基准, 硬盘首扇区相对号(高位字节在后)
C～F	总扇区数	分区所占用实际扇区数(高位字节在后)

3 主引导记录的查看及修改

可以使用BIOS 功能调用“INT13”, 将硬盘的 0 面 0 道 1 号扇区的 512 个字节, 调入内存指定位置, 进行查看或修改, 并把修改后的结果再存入到硬盘的 0 面 0 道 1 扇区, 以达到修正主引导记录的目的. 当然也可以采用其他方法, 如利用 PCTOOLS 查看硬盘的主引导记录, 但没有此方法简单, 特别是修改时更是如此. 硬盘的BIOS 中断调用方法如下:

用DOS 的DEBUG 命令编写一段读取硬盘主引导记录的汇编程序.

```
-A 100 ; 从内存偏移地址 100 处开始编程.
MOV AX, 0201      ; 02 表示读硬盘, 01 表示对一个扇区操作.
MOV BX, 200       ; 将 512 个字节读入到内存 200 开始的连续 512 个单元中.
MOV CX, 0001      ; 开始扇区号为 1.
MOV DX, 0080      ; 指定对C 盘操作.
INT 13            ; BIOS 中断调用.
-G= 100, 10E      ; 执行以上这段程序.
```

执行完上述这段程序后, 硬盘的 0 面 0 道 1 扇区的 512 个字节就被调入内存. 要查看主引导记录, 键入“D 200”, 若要查看硬盘分区信息键入“D 3BE”. 下面为某一硬盘分区信息:

××××: 03B0	80 01
××××: 03C0	01 00 06 04 D1 02 11 00- 00 00 EE FF 00 00

其意义为: 80= 可自举; (01 01 00)= 分区起始位置在 01 头 01 扇区 00 柱面; 06= DOS 3. 3 以上版本; (04 D1 02)= 分区终止位置在 04 头D1 扇区 02 柱面; (11 00 00 00)= 本分区起始相对扇区为"00 00 00 11"; (EE FF 00 00)= 分区实用扇区总数为"00 00 FF EE"(即 65618 个扇区).

若硬盘主引导记录(包括分区表)被破坏, 可对照正确的主引导记录数据, 用DEBUG 的 E 命令进行修正. 最后将修正好的引导记录写回到硬盘.

方法是只要把上面程序的第一条改为: "MOV AX, 0301"(03= 写硬盘, 01= 对 1 个扇区操作), 其他相同. 当执行完该段程序后, 修正好的主引导记录就被写回到硬盘的 0 面 0 道 1 扇区.

4　重建主引导记录的原理和方法

通过上述对主引导记录的分析, 可得出修正主引导记录的方法:

(1) 预先备份主引导记录, 可直接对被破坏的主引导记录进行修正.

(2) 对于硬盘分区表, 可以通过计算的方法来重建被破坏的分区表.

然而第一种方法必须事先有主引导记录备份, 第二种方法非常麻烦, 容易出错. 那么能否使用广大用户所熟悉的 FDISK. COM 命令来重建主引导记录? 显然是可以的, 但是问题就在于 FDISK 在重建过程中, 会彻底破坏硬盘原有的所有数据. 这是由于它在创建过程中, 要对DOS 的引导区, FAT 区及文件目录区进行写零操作, 以保证 FORMAT. COM 能顺利进行格式化. 因此若能在创建过程中, 阻止其对除主引导记录区外所有的写零操作, 就能在不破坏硬盘原有数据的情况下, 使用 FDISK. COM 来重建硬盘主引导记录.

由上述分析可知, 在运行 FDISK. COM 命令之前, 先运行一段驻留程序, 它具体的功能就是截取读写硬盘的 13H 号中断向量, 取消所有对硬盘主引导记录区以外的所有写操作. 然后再用FDISK. COM 命令, 这样就能实现重建硬盘主引导记录, 又不破坏原有的硬盘数据.

该驻留汇编原程序如下:

```
CODE SEGMENT
        ASSUME CS: CODE, DS: CODE, ES: CODE
        ORG 100H
MAIN:   JMP START
        INT13 DB 04H DUP(0)
; 指定可以进行写操作的硬盘空间.
RECD:   CMP AH, 05H
        JNZ CHKET
CHANG:MOV AH, 00H
CHKET:  CMP AH, 03H
        JNZ GOOD
        CMP AX, 0301H
```

```
        JNZ CHANG
        CMP CX, 0001H
        JNZ CHANG
        CMP DX, 0080H
        JNZ CHANG
; 调用子程序.
GOOD:   PUSHF
        CALL CS:DWORD PRT[INT13]
        IRET
        START JMP START1
        DISP DB 0DH, 0AH, 'Program has done',
        0DH, 0AH, 24H
; 截取原 13 号中断向量.
START1:MOV AX, 3513H
        INT 21H
; 保存原 13 号中断向量.
        MOV CS:WORD PRT[INT13], BX
        MOV AX, ES
        MOV CS:WORD PRT[INT13+ 02H], AX
        CLI          ; 关闭中断.
; 指定 RECD 开始的程序作为新的 13 号中断向量.
        MOV AX, CS
        MOV DS, AX
        LEA DX, RECD
        MOV AX, 2513H
        INT 21H
        STI          ; 开启中断.
; 程序驻留内存并显示提示信息.
        LEA DX, DISP2
        MOV AH, 09H
        INT 21H
        INT 27H
        CODE ENDS
        END BEGIN
```

本段驻留程序的核心就是利用 BIOS 的 13H 号硬盘中断调用, 来指定硬盘进行写零操作的区域. 由于它已获取 13H 号中断向量, 同时又是常驻内存, 所以当运行 FDISK. COM 命令时, 会自动先运行该段驻留程序(指定只允许对 0 面 0 道 1 扇区进行写操作), 然后再执行分区命令, 这样就能实现既建立分区创建硬盘主引导记录, 又不破坏原有硬盘数据.

参 考 文 献

1　Peter Norton. Inside The PC. New York: Prentice Hall Brady, 1993
2　为林, 维钢. 386/486 维修调试与中断调用速查. 北京: 学苑出版社, 1994
3　唐华栋, 等. 新编维修大全. 北京: 海洋出版社, 1992

Rebuilding Data of Hard Disk Main Boot Record

Xin Genyong
(Laboratory Administrate)

Abstract　This article introduce the structure of boot record and Partition table of a Hard Disk and a method of checking and modifying the Hard Disk boot record. More discuss is given to the principle and the method about how to rebuild the boot record without destroying the originally date hold in the Hard Disk.

Key words　boot record; partition table; interrupt vector; reserved program