

文件系统

文件系统整体结构

文件系统是操作系统用于明确磁盘或分区上的文件的方法和数据结构；即在磁盘上组织文件的方法.在移动存储设备上比较常用的有FAT文件系统和ExFAT文件系统。

FAT分区依据FAT表中每个簇链的所占位数分为fat12、fat16、fat32三种格式；

exFAT是为了解决FAT32等不支持4G及其更大的文件而推出的文件系统。

知识点

bios

bios(basic input output system),他是一组固化在计算机主板上ROM芯片上的程序,保存着计算机最重要的基本输入输出程序,开关机自荐程序和系统自启动程序.他可以从CMOS上读写系统设置的具体信息,主要为计算机提供最底层,最直接的硬件设置和控制.

MBR扇区

MBR(master boot record)即主引导扇区(或记录),位于整个硬盘的0柱面0磁头1扇区(即硬盘的第一个扇区),
bios在执行完自己固有的程序后会jump到MBR的第一条指令,并将系统的控制权交由MBR,总共1个扇区的主引导记录,MBR引导程序战前446字节(0h~1bdh),
随后的64字节(1beh~1fdh)为DPT(disk partitiontable),最后为"55 aa"结束符.
MBR具有公共引导的特性,与具体的操作系统无关,具有唯一性.

簇

指可分配用来保存文件的最小磁盘空间，一个簇只能存放一个文件的内容。因此，文件所占用的空间应该是簇的整数倍。簇的大小会影响磁盘文件的排列，设置过大可以减少磁盘碎片但是会影响存储效率；设置过小虽然可以增强存储效率但是会产生大量的磁盘碎片。因此一个簇的大小一般为4kb(兼顾双方，取其适中)。

名词解释

FAT : File Allocation Table.文件分配表
EXFAT: Extended File Allocation Table .扩展文件分配表
BPB: BIOS Parameter block.BIOS参数块
BS: Boot Sector.启动扇区

LSN:	Logical Sector Number.逻辑扇区号
PSN:	Physical Sector Number.物理扇区号
LBA:	Logical Block Address.逻辑块地址

FAT12

采用12位文件分配表
最大簇总数4085 (2的12次方)
最大分区容量8M (4096clusters × 4sectors/clusters × 512bytes/sectors)
只能是8.3格式的文件名 (短名)

FAT16

采用16位的文件分配表
最大簇总数65524 (2的16次方)
最大分区容量2G
严重缺陷: 大容量磁盘利用效率低

FAT32

采用32位的文件分配表
最大簇总数 (2的32次方)
单个文件不能大于4G
当分区小于512M时, Fat32不会发生作用
不超过8GB的分区中, FAT32分区格式的每个簇都固定为4KB
Fat32不能保持向下兼容

注: 可以通过WinHex查看磁盘分区信息

FAT表数据结构

FAT表是一一对应于数据区簇号的列表, 文件系统分配磁盘空间是按簇来分配,因此, 文件占用磁盘空间时, 基本单位是簇。
FAT表是根据簇数来和文件对应的。第一个存放数据的簇是簇2。
FAT表项的大小与FAT类型有关, FAT12的表项为12-bit,FAT16为16-bit,FAT32则为32-bit。
FAT32的FAT表项只有28-bit可以使用, 所以他的高4位保留。FAT32在扇区号为6的地方完整地拷贝了一份启动扇区的备份, 包括BPB的内容。

FATType的判定条件

FAT类型 (FATType) 的检测 (是FAT12, 或是FAT16, 还是FAT32) 只能通过计算FAT卷中数据区所占的簇数 (CountofClusters) 来判定, 没有其他办法。

FAT目录结构

对于FAT12/FAT16，根目录存储在磁盘中固定的地方，它紧跟在最后一个FAT表后。根目录的扇区数也是固定的，可以根据**BPB_RootEntCnt**计算得出。

FAT32的根目录由簇链组成，其扇区数不确定，根目录的第一个扇区号存储在**BPB_RootClus**中，根目录不同于其他的目录，没有日期和时间戳，也没有目录名，同时根目录里没有“.”和“..”这两个目录项。根目录另一个特殊的地方在于，根目录中有一个设置 **ATTR_VOLUME_ID** 位的文件，这个文件在整个FAT卷中是唯一的。

FAT的32-byte 目录项结构

DIR_NTRes:

当文件只有短名时，该短名的大小写规则如下：

1. 此值为18H时，文件名和扩展名都小写。
2. 此值为10H时，文件名大写而扩展名小写。
3. 此值为08H时，文件名小写而扩展名大写。
4. 此值为00H时，文件名和扩展名都大写。

DIR_Attr:

DIR_Attr

长名与短名规则

短文件名（8+3name）是FAT16遗留下来的，为了兼容windows以后的版本文件和目录都有长名和短名。

长名目录项和对应的别名（短名）目录项的存储有以下6个处理原则：

1. 取长文件名的前6个字符加上“~1”形成长文件名的别名（即短文件名），并将长文件名中最后一部分（最后一个间隔符“.”后面字符）的前3个字符作为其扩展名。
2. 如果已存在这个名字的文件，则符号“~”后的数字会自动增加
3. 任何包括小写字母的文件名都被看作是长文件名，而不管其长度是多少。
4. 长文件名存储在属性标志为0FH的32字节目录登记项中（这是与短文件名目录项的区别）。用Unicode格式编码，每个字符（无论是英文或是汉字）均占2字节。
6. 每个目录登记项用26个字节存储13个字符（序号由第1字节指定）。位置多余时，先用00h表示结束，再用FFh填充。
7. 长文件名用若干个长名目录项保存，长文件名目录项倒序排在文件短目录项前面。

Windows9x会根据应用程序的性质分别给予不同的文件名，16位应用程序得到8.3格式的文件名，而32位应用程序得到长文件名。

注：尽量不要在根目录下创建长文件名！

FAT计算公式

根目录所占的扇区数(RootDirSectors):

```
RootDirSectors = ((BPB_RootEntCnt * 32) + (BPB_BytePerSec - 1)) / BPB_BytePerSec;
```

数据区的起始地址(FirstDataSector)：

```
FirstDataSector = BPB_RsvdSecCnt + (BPB_NumFATs * FATSz) + RootDirSectors;
```

其中，FATSz可以由下面条件获取：

```
If(BPB_FATSz16 != 0)
    FATSz = BPB_FATSz16;
Else
    FATSz = BPB_FATSz32;
```

由于每一个存放数据的簇是簇2，所以数据区的起始地址也相当于簇2的起始地址，由此可以得到下面的一个计算公式。

给一个合法的簇号N(N>=2),可以由该簇号计算得出该簇的每一个扇区号：

```
FirstSectorofCluster = ( (N - 2) * BPB_SecPerClus + FirstDataSector)
```

数据区中的扇区数(DataSec)：

```
DataSec = TotSec - FirstDataSector;
```

其中，TotSec可以由下面条件获取：

```
If(BPB_TotSec16 != 0)
    TotSec = BPB_TotSec16;
Else
    TotSec = BPB_TotSec32;
```

数据区中的总簇数 (CountofClusters)：

```
CountofClusters = DataSec / BPB_SecPeClus;
```

某个簇号在FAT表中的位置：

A)簇N在第一个FAT表中的扇区数 (ThisFATSecNum)：

```
ThisFATSecNum = BPB_RsvdSecCnt + (FATOffset / BPB_BytePerSec);
```

其中FATOffset可以由下面条件获取：

```
If(FATType == FAT16)
{
    FATOffset = N*2;
}
Else If(FATType == FAT32)
{
    FATOffset = N*4;
}
```

B)簇N在第一个FAT表中所在扇区的偏移 (ThisFATEntOffset)：


```
ThisFATEntOffset = FATOffset % BPB_BytePerSec;
```

***注：以上的计算结果都是四舍五入的。**

EXFAT

单个文件大小突破4GB的限制，最大可达到32GB、
分区大小突破之前32GB的限制，最大可达到2TB。
内部结构调整，实现同样功能的操作，相比较之前的FAT系统，减少读写设备的次数。
对DBR表，文件名，文件目录项等，增加校验字段，提高数据安全性。
簇大小可高达32MB。
采用了剩余空间分配表，剩余空间分配性能改进。
同一目录下最大文件数可达65535个。

exfat文件系统内部结构分配如下：

 exfat文件系统内部结构

Exfat的Boot区最少为24个扇区，分成BOOT区和备份BOOT区，两个区各12个扇区。

跳转指令 **EB 76 90** 也是EXFAT的type识别码

EXFAT目录

根目录比较特殊，下面有三个特殊的目录项。具体如下：

其中第一个目录项不知道有何具体用意。
第二个目录项0x81，表示簇堆分配表文件。
第三个目录项0x82，表示大写表文件。
EXFAT普通目录下没有“.”和“..”目录项。
特殊目录项只存在根目录下，有卷标目录项、位映射目录项和大写表目录项，分别记录分区卷标，簇堆分配表文件和大写表文件。

EXFAT簇堆分配表

簇堆分配表，记录分区上所有簇的使用情况。每一个bit代表一个簇，0表示空簇，1表示该簇已被占用。起始簇号从2开始，也就是BIT0对应簇号2，BIT1对应簇号3。簇堆分配表以文件存储的方式存在，一般对应根目录下第一个文件，也就是第二个目录项。他的大小由总簇数决定，占用N个簇的空间。

EXFAT大写转换表

大写表是一张Unicode字符映射图，每一个字符占用2个字节。文件名比较时，先把文件名格式转换成Unicode，再通过该表把文件名转成大写Unicode，转换完成后才进行文件名比较。大写表中的数据进行了部分压缩，压缩起始标志码FFFFh，随后跟一个压缩长度。

注：硬盘的物理结构

 磁盘结构图