FAT12简介

钱宇辰

1767855130@qq.com

起源

- FAT（File Allocation Table）文件系统在DOS v1.0时代就引入了，是最基本的文件系统之一。

- FAT家族：FAT12、FAT16、FAT32、ExFAT、VFAT

FAT12

- 12位地址，最大容量16MB
- 为软盘设计的文件系统

FAT结构

- FAT文件系统把存储介质看成一维的数组，基本单位是簇（cluster）。存储介质被划分为3个区域：boot record、FAT、directory and data area。

- 一个簇包含一个扇区，大小为512B。

FAT结构（续）

Boot record

- 引导扇区包含了数据和代码，数据被称为BPB（BIOS Parameter Block）

Offset (decimal)	Offset (hex)	Size (in bytes)	Meaning
0	0x00	3	The first three bytes EB 3C 90 disassemble to JMP SHORT 3C NOP. (The 3C value may be different.) The reason for this is to jump over the disk format information (the BPB and EBPB). Since the first sector of the disk is loaded into ram at location 0x0000:0x7c00 and executed, without this jump, the processor would attempt to execute data that isn't code. Even for non-bootable volumes, code matching this pattern (or using the E9 jump opcode) is required to be present by both Windows and OS X. To fulfil this requirement, an infinite loop can be placed here with the bytes EB FE 90.
3	0x03	8	OEM identifier. The first 8 Bytes (3 - 10) is the version of DOS being used. The next eight Bytes 29 3A 63 7E 2D 49 48 and 43 read out the name of the version. The official FAT Specification from Microsoft says that this field is really meaningless and is ignored by MS FAT Drivers, however it does recommend the value "MSWIN4.1" as some 3rd party drivers supposedly check it and expect it to have that value. Older versions of dos also report MSDOS5.1, linux-formatted floppy will likely to carry "mkdosfs" here, and FreeDOS formatted disks have been observed to have "FRDOS5.1" here. If the string is less than 8 bytes, it is padded with spaces.
11	0x0B	2	The number of Bytes per sector (remember, all numbers are in the little-endian format).
13	0x0D	1	Number of sectors per cluster.
14	0x0E	2	Number of reserved sectors. The boot record sectors are included in this value.

每个扇区的字节数

每个簇的扇区数

Boot record占用的扇区数

Boot record（续）

16	0x10	1	Number of File Allocation Tables (FAT's) on the storage media. Often this value is 2.	FAT的数量，一般为2
17	0x11	2	Number of directory entries (must be set so that the root directory occupies entire sectors).	根目录文件数的最大值
19	0x13	2	The total sectors in the logical volume. If this value is 0, it means there are more than 65535 sectors in the volume, and the actual count is stored in the Large Sector Count entry at 0x20.	扇区数
21	0x15	1	This Byte indicates the media descriptor type.	
22	0x16	2	Number of sectors per FAT. FAT12/FAT16 only.	FAT表的数量
24	0x18	2	Number of sectors per track.	
26	0x1A	2	Number of heads or sides on the storage media.	
28	0x1C	4	Number of hidden sectors. (i.e. the LBA of the beginning of the partition.)	
32	0x20	4	Large sector count. This field is set if there are more than 65535 sectors in the volume, resulting in a value which does not fit in the *Number of Sectors* entry at 0x13.	

Boot record（续）

36	0x024	1	Drive number. The value here should be identical to the value returned by BIOS interrupt 0x13, or passed in the DL register; i.e. 0x00 for a floppy disk and 0x80 for hard disks. This number is useless because the media is likely to be moved to another machine and inserted in a drive with a different drive number.
37	0x025	1	Flags in Windows NT. Reserved otherwise.
38	0x026	1	Signature (must be 0x28 or 0x29).
39	0x027	4	VolumeID 'Serial' number. Used for tracking volumes between computers. You can ignore this if you want.
43	0x02B	11	Volume label string. This field is padded with spaces.
54	0x036	8	System identifier string. This field is a string representation of the FAT file system type. It is padded with spaces. The spec says never to trust the contents of this string for any use.
62	0x03E	448	Boot code.
510	0x1FE	2	Bootable partition signature 0xAA55.

Boot代码

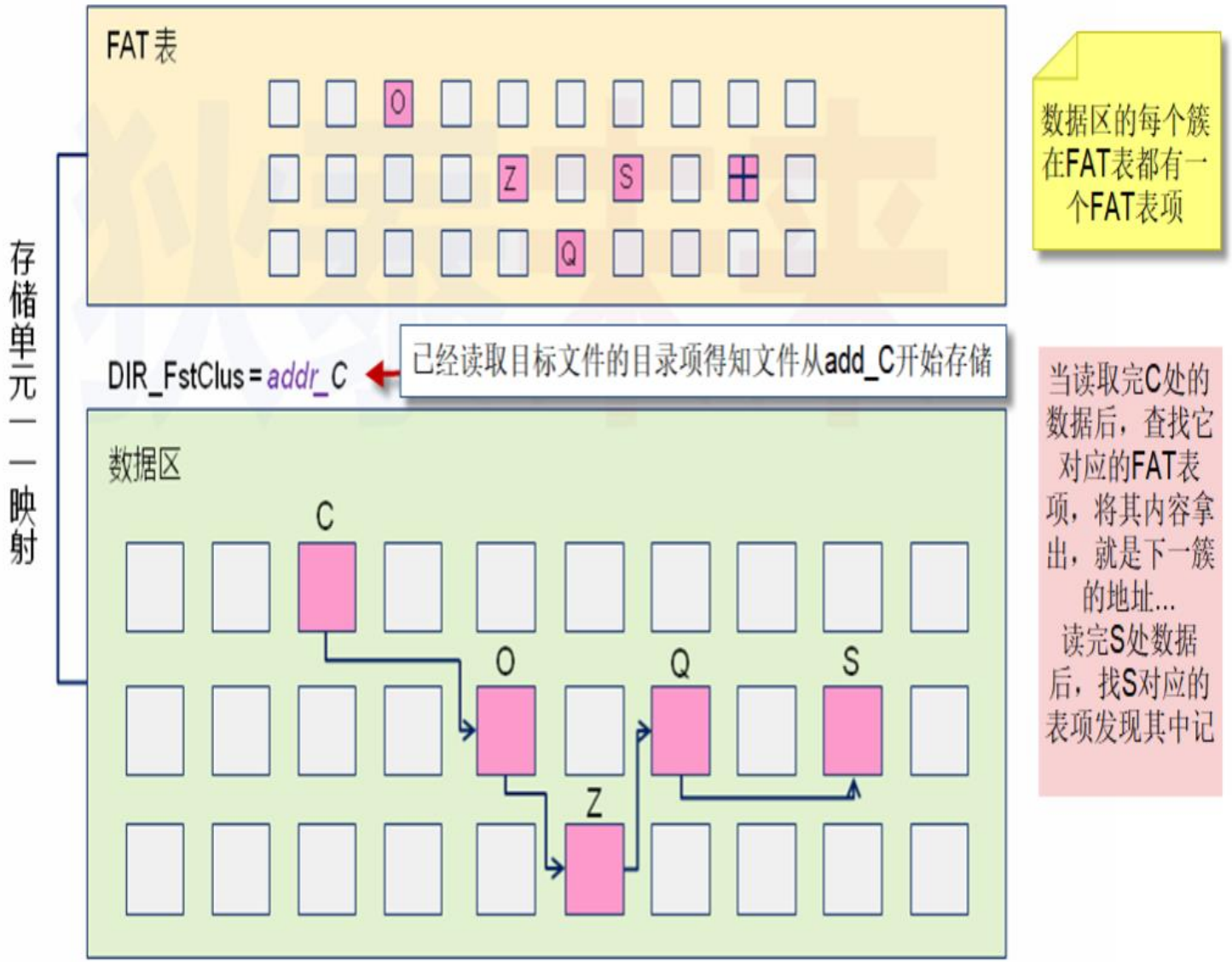
Magic number 0xAA55

Boot record占据了第一个扇区！

File Allocation Table

- FAT1和FAT2互为备份。
- 文件分配表被划分为紧密排列的若干个表项，每个表项都与数据区中的一个簇相对应，而且表项的序号也是与簇号一一对应的。
- 每12位成为一个FAT项(FATEntry)，代表一个簇。所以2个FAT项会占用3个字节
- 在1.44M软盘上，FAT前三个字节的值是固定的0xF0、0xFF、0xFF，用于表示这是一个应用在1.44M软盘上的FAT12文件系统。本来序号为0和1的FAT表项应该对应于簇0和簇1，但是由于这两个表项被设置成了固定值，簇0和簇1就没有存在的意义了，**所以数据区就起始于簇2。**
- FAT项的值代表文件的下一个簇号
  - 值大于或等于0xFF8，表示当前簇已经是本文件的最后一个簇
  - 值为0xFF7，表示它是一个坏簇

File Allocation Table（续）



Directory area

- 根目录区由目录项（entry）组成，一个目录项占32个字节。

Offset (in bytes)	Length (in bytes)	Meaning
0	11	8.3 file name. The first 8 characters are the name and the last 3 are the extension.
11	1	Attributes of the file. The possible attributes are: `READ_ONLY=0x01 HIDDEN=0x02 SYSTEM=0x04 VOLUME_ID=0x08 DIRECTORY=0x10 ARCHIVE=0x20 LFN=READ_ONLY|HIDDEN|SYSTEM|VOLUME_ID` (LFN means that this entry is a long file name entry)
12	1	Reserved for use by Windows NT.
13	1	Creation time in tenths of a second. Range 0-199 inclusive. Based on simple tests, Ubuntu16.10 stores either 0 or 100 while Windows7 stores 0-199 in this field.

Directory area（续）

<table>
<tr><td>14</td><td>2</td><td>The time that the file was created. Multiply Seconds by 2.<table><tr><td>Hour</td><td>5 bits</td></tr><tr><td>Minutes</td><td>6 bits</td></tr><tr><td>Seconds</td><td>5 bits</td></tr></table></td></tr>
<tr><td>16</td><td>2</td><td>The date on which the file was created.<table><tr><td>Year</td><td>7 bits</td></tr><tr><td>Month</td><td>4 bits</td></tr><tr><td>Day</td><td>5 bits</td></tr></table></td></tr>
<tr><td>18</td><td>2</td><td>Last accessed date. Same format as the creation date.</td></tr>
<tr><td>20</td><td>2</td><td>The high 16 bits of this entry's first cluster number. For FAT 12 and FAT 16 this is always zero.</td></tr>
<tr><td>22</td><td>2</td><td>Last modification time. Same format as the creation time.</td></tr>
<tr><td>24</td><td>2</td><td>Last modification date. Same format as the creation date.</td></tr>
<tr><td>26</td><td>2</td><td>The low 16 bits of this entry's first cluster number. Use this number to find the first cluster for this entry.</td></tr>
<tr><td>28</td><td>4</td><td>The size of the file in bytes.</td></tr>
</table>

Directory area（续）

- 如果文件名过长，在原本的目录项后面会立即跟一个LFN项，同样也是32个字节。

Offset (in bytes)	Length (in bytes)	Meaning
0	1	The order of this entry in the sequence of long file name entries. This value helps you to know where in the file's name the characters from this entry should be placed.
1	10	The first 5, 2-byte characters of this entry.
11	1	Attribute. Always equals 0x0F. (the long file name attribute)
12	1	Long entry type. Zero for name entries.
13	1	Checksum generated of the short file name when the file was created. The short filename can change without changing the long filename in cases where the partition is mounted on a system which does not support long filenames.
14	12	The next 6, 2-byte characters of this entry.
26	2	Always zero.
28	4	The final 2, 2-byte characters of this entry.

Data area

- 数据区的第一个簇的簇号是2，为什么？
- 数据区开始扇区号=根目录开始扇区号+根目录所占扇区数。
- 若为目录，格式同根目录项。

reference

- https://wiki.osdev.org/FAT#File_Allocation_Table
- https://blog.csdn.net/qq_39654127/article/details/88429461#main-toc