唐佐林视频教程

狄泰未来

第4课

主引导程序的扩展（上）

主引导程序的扩展

- 限制

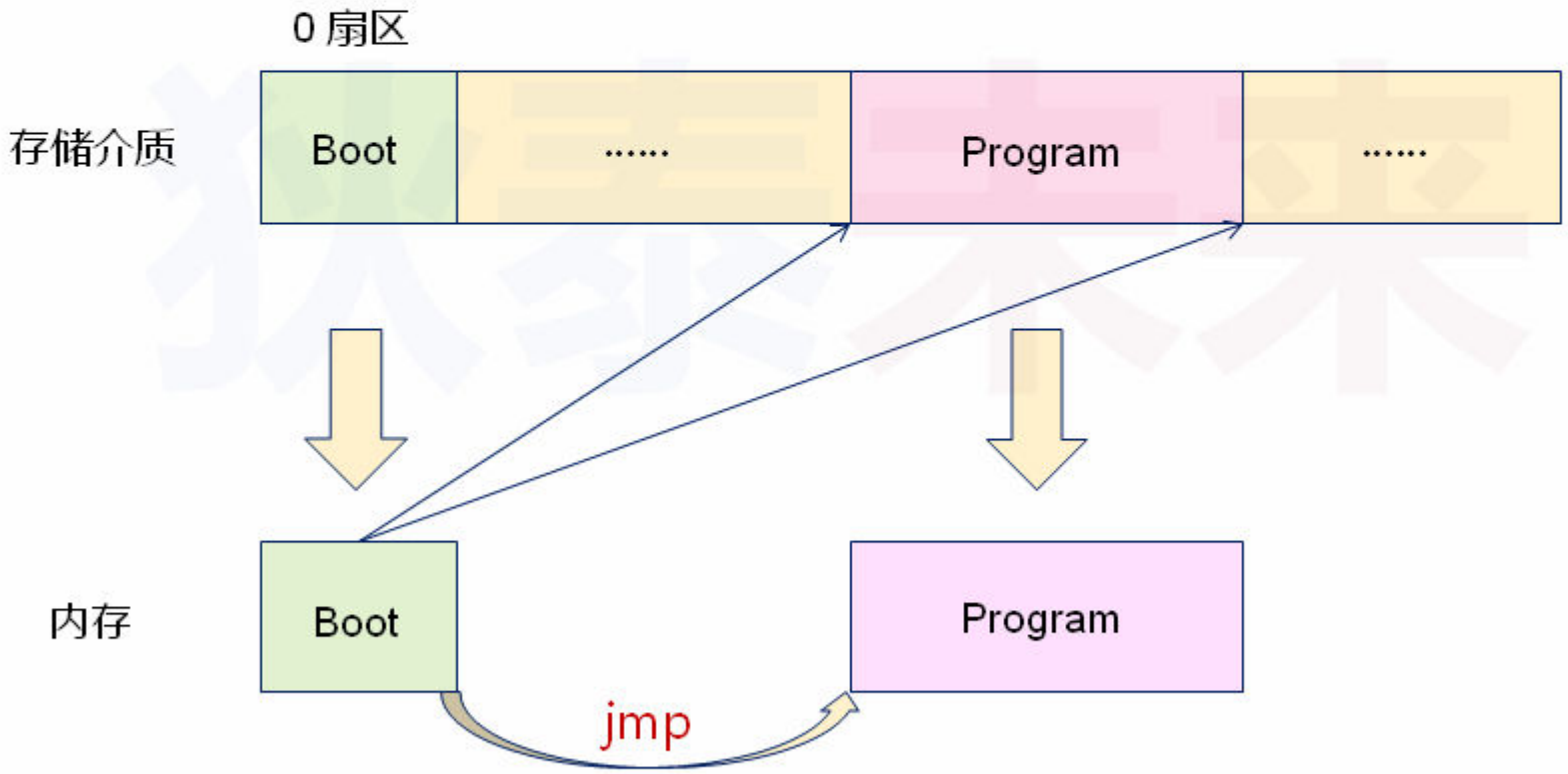
主引导程序的代码量不能超过 512 字节！！

主引导程序的扩展

- 突破限制的思路
  - 主引导程序
    1. 完成最基本的初始化工作
    2. 从存储介质中加载程序到内存中
    3. 将控制权交由新加载的程序执行
    4. ……

主引导程序的扩展

- 突破限制的思路



主引导程序的扩展

- 问题

主引导程序如何加载存储介质中的其它程序？

主引导程序的扩展

- 文件系统
  - 存储介质上组织文件数据的方法（数据组织的方式）

FAT12文件格式

主引导程序的扩展

- 文件系统示例
  - FAT12 是 DOS 时代的早期文件系统
  - FAT12 结构非常简单，一直沿用于软盘
  - FAT12 的基本组织单位
    - 字节（Byte）：基本数据单位
    - 扇区（Sector）：磁盘中的最小数据单元
    - 簇（Cluster）：一个或多个扇区

主引导程序的扩展

- 解决方案
  - 使用 FAT12 对软盘（data.img）进行格式化
  - 编写可执行程序（Loader），并将其拷贝到软盘中
  - 主引导程序（Boot）在文件系统中查找 Loader
  - 将 Loader 复制到内存中，并跳转到入口处执行

主引导程序的扩展

- 实验： 往虚拟软盘中写入文件
  - 原材料： FreeDos， Bochs， bximage
  - 步骤：
    - 创建虚拟软盘 data.img
    - 在 FreeDos 中进行格式化（FAT12）
    - 将 data.img 挂载到 Linux 中，并写收入文件

编程实验

将文件写入虚拟软盘

主引导程序的扩展

- 下一步的工作

Boot 查找目标文件（Loader），并读取文件的内容！

主引导程序的扩展

- 深入 FAT12 文件系统

FAT12文件系统由引导区，FAT表，根目录项表和文件数据区组成。

扇区位置	长度	内容
0	1 (512 B)	引导程序
1	9 (4608 B)	FAT 表 1
10	9 (4608 B)	FAT 表 2
19	14 (9728 B)	目录文件项
33	----	文件数据

主引导程序的扩展

- FAT12 的主引导区

主引导区存储的比较重要的信息是文件系统的类型，文件系统逻辑扇区总数，每簇包含的扇区数，等。主引导区最后以 0x55AA 两个字节作为结束，共占用一个扇区。

主引导程序的扩展

标识	偏移量	类型	大小	默认值	说明
BS_JmpBoot	0	db	3		跳转指令
BS_OEMName	3	db	8	MSWIN4.1	OEM字符串，必须为8个字符，不足以空格填空
BPB_BytsPerSec	11	dw	2	0x200	每扇区字节数
BPB_SecPerClus	13	db	1	1	每簇占用的扇区数
BPB_RsvdSecCnt	14	dw	2	1	Boot占用的扇区数
BPB_NumFATs	16	db	1	2	FAT表的记录数
BPB_RootEntCnt	17	dw	2	0xE0	最大根目录文件数
BPB_TotSec16	19	dw	2	0xB40	逻辑扇区总数
BPB_Media	21	db	1	0xF0	媒体描述符
BPB_FATSz16	22	dw	2	9	每个FAT占用扇区数
BPB_SecPerTrk	24	dw	2	0x12	每个磁道扇区数
BPB_NumHeads	26	dw	2	2	磁头数
BPB_HiddSec	28	dd	4	0	隐藏扇区数
BPB_TotSec32	32	dd	4	0	如果BPB_TotSec16是0，则在这里记录扇区总数
BS_DrvNum	36	db	1	0	中断13的驱动器号
BS_Reserved1	37	db	1	0	未使用
BS_BootSig	38	db	1	0x29	扩展引导标志
BS_VolID	39	dd	4	0	卷序列号
BS_VolLab	43	db	11		卷标，必须是11个字符，不足以空格填充
BS_FileSysType	54	db	8	FAT12	文件系统类型，必须是8个字符，不足填充空格
BOOT_Code	62	db	448	0x00	引导代码，由偏移0字节处的短跳转而来
END	510	db	2	0x55, 0xAA	系统引导标识

主引导程序的扩展

- 实验： 读取 data.img 中的文件系统信息
  - 步骤：
    - 创建 Fat12Header 结构体类型
    - 使用文件流读取前 512 字节的内容
    - 解析并打印相关的信息

编程实验

读取 FAT12 文件系统信息

主引导程序的扩展

- 实验结论

1. FreeDos 中的 format 程序在格式化软盘的时候自动在第 0 扇区生成了一个主引导程序，这个主引导程序只打印一个字符串
2. 文件格式和文件系统都是用于定义数据如何存放的规则，只要遵循这个规则就能够成功读写目标数据

小结

- 主引导程序的代码量不能超过 512 字节
- 可以通过主引导程序加载新程序的方式突破限制
- 加载新程序需要依赖于文件系统
- FAT12 是一种早期用于软盘的简单文件系统
- FAT12 文件系统的重要信息存储于 0 扇区