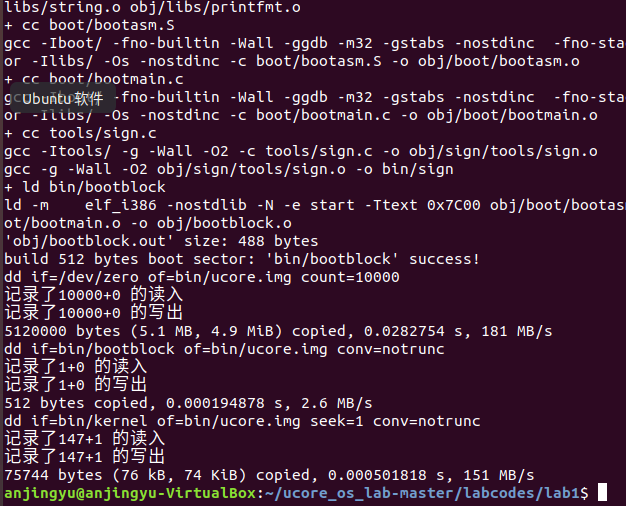
练习1：理解通过make生成执行文件的过程。（要求在报告中写 出对下述问题的回答）

列出本实验各练习中对应的OS原理的知识点，并说明本实验中的实现部分如何对应和体现了 原理中的基本概念和关键知识点。

在此练习中，大家需要通过静态分析代码来了解：

1. 操作系统镜像文件ucore.img是如何一步一步生成的？(需要比较详细地解释Makefile中每 一条相关命令和命令参数的含义，以及说明命令导致的结果) 能

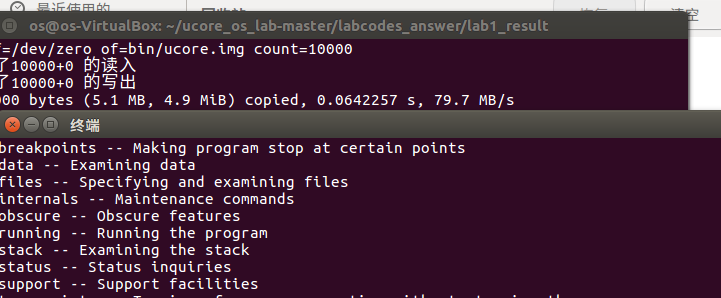
显示了想要生成uore.img需要先生成bootlock

1. 一个被系统认为是符合规范的硬盘主引导扇区的特征是什么？

引导扇区的大小为512字节，最后两个字节为标准性结束字节0x55,0xAA，做完这样的检查才能认为是符合规范的磁盘主引导扇区

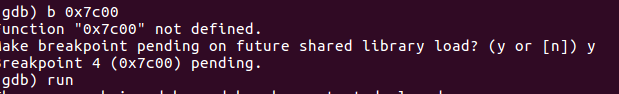
练习2：使用qemu执行并调试lab1中的软件。（要求在报告中简 要写出练习过程）

为了熟悉使用qemu和gdb进行的调试工作，我们进行如下的小练习：

1. 从CPU加电后执行的第一条指令开始，单步跟踪BIOS的执行。
2.  2. 在初始化位置0x7c00设置实地址断点,测试断点正常。

3. 从0x7c00开始跟踪代码运行,将单步跟踪反汇编得到的代码与bootasm.S和 bootblock.asm进行比较。

4. 自己找一个bootloader或内核中的代码位置，设置断点并进行测试。



练习3：分析bootloader进入保护模式的过程。（要求在报告中 写出分析）

BIOS将通过读取硬盘主引导扇区到内存，并转跳到对应内存中的位置执行bootloader。请分 析bootloader是如何完成从实模式进入保护模式的。

提示：需要阅读小节“保护模式和分段机制”和lab1/boot/bootasm.S源码，了解如何从实模式 切换到保护模式，需要了解：

为何开启A20，以及如何开启A20 如何初始化GDT表 如何使能和进入保护模式

***从实模式进入保护模式只需要经历三个步骤，第一步加载gdt第二部，，打开A20,第三部置ro为1，开启A20的原因是在保护模式下如果A20开启可以访问连续内存，关闭就只能访问偶数内存。当A20地址线控制禁止时，则程序就像在8086中运行，1M以上的地址是不可访问的。开启A20有3种方法1.通过键盘控制器。2.通过BIOS提供的中断。3.通过系统的I/O端口。初始化GDT：lggt gdtdesc***

***Mov1 %cr0,%eax***

***Orl $CR0\_PE\_ON,%eax***

***Movl %eax,%cr0***

练习4：分析bootloader加载ELF格式的OS的过程。（要求在报 告中写出分析）

通过阅读bootmain.c，了解bootloader如何加载ELF文件。通过分析源代码和通过qemu来运 行并调试bootloader&OS，

bootloader如何读取硬盘扇区的？ bootloader是如何加载ELF格式的OS？

提示：可阅读“硬盘访问概述”，“ELF执行文件格式概述”这两小节bootmain第一行***readseg((uintptr\_t)ELFHDR, SECTSIZE \* 8, 0);读取了位于主引导扇区的后的连续8个扇区放到ELFHDR处ELFHDR是0x100000,然而kernel.ld`中描述了内核的位置也是0x100000***