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）

(1)通过GCC编译器将Kernel目录下的.c文件编译成OBJ目录下的.o文件。

(2)ld命令根据链接脚本文件kernel.ld将生成的\*.o文件，链接成BIN目录下的kernel文件

(3)通过GCC编译器将boot目录下的.c,.S文件以及tools目录下的sign.c文件编译成OBJ目录下的\*.o文件。

(4)ld命令将生成的\*.o文件，链接成BIN目录下的bootblock文件。

(5)dd命令将dev/zero, bin/bootblock,bin/kernel 写入到bin/ucore.img

练习**2**：使用**qemu**执行并调试**lab1**中的软件。（要求在报告中简

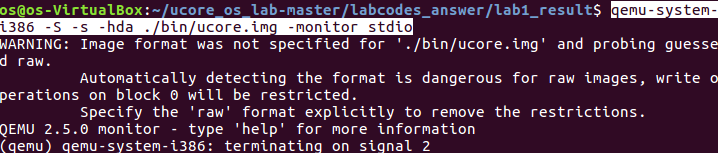
要写出练习过程）

(1)打开一个终端进入lab1\_answer的路径,输入qemusystem-

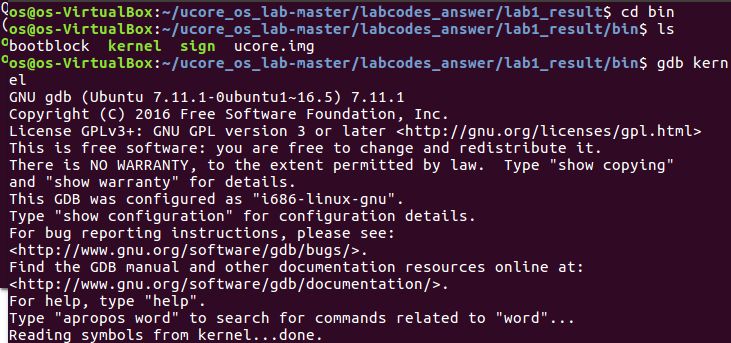
i386 -S -s -hda ./bin/ucore.img -monitor stdio命名将虚拟机跑你来并等待调试操

作。项目中有两个可执行文件（obj/bootblock.o bin/kernel），一个对应于bootLoader，一个对应

于操作系统内核，可以选择任意一个进行调试。



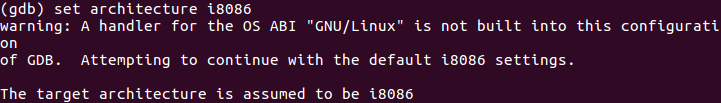
（2）在另一个窗口键入 i386-elf-gdb + 需要调试的文件



（3）入gdb后，键入 target remote 127.0.0.1:1234 ,使得gdb与qemu连接。

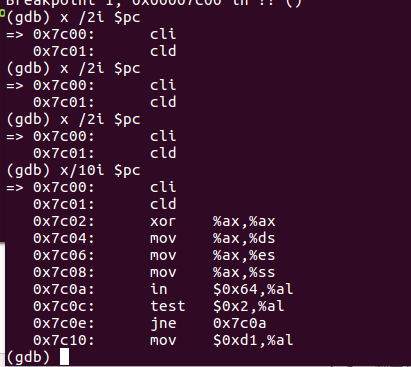


（4）然后就可以开始调试了。



（5）b + 函数名 或者 内存地址 ： 表示添加断点





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，bootloader主要功能：

切换到保护模式，启用分段机制；读磁盘中ELF执行文件格式的ucore操作系统到内存；显示字符串；把控制权交给ucore操作系统；

代码执行到0x7c00处，进行以下操作

**1.清理环境：将flag置0和将段寄存器置0**

**2.开启A20：通过将键盘控制器上的A20线置于高电位，全部32条地址线可用，可以访问4G的内存空间**

**3.初始化GDT表：一个简单的GDT表和其描述符已经静态储存在引导区中，载入即可；**

**4.进入保护模式：通过将cr0寄存器PE位置1便开启了保护模式；**

movl %cr0, %eax

orl $CR0\_PE\_ON, %eax

movl %eax, %cr0

.set CR0\_PE\_ON, 0x1

**5.通过长跳转更新cs的基地址；**

**# Jump to next instruction, but in 32-bit code segment.**

**# Switches processor into 32-bit mode.**

**ljmp $PROT\_MODE\_CSEG, $protcseg**

**.set PROT\_MODE\_CSEG, 0x8**

**6.设置段寄存器，并建立堆栈；**

.set PROT\_MODE\_DSEG, 0x10

protcseg:

# Set up the protected-mode data segment registers

movw $PROT\_MODE\_DSEG, %ax # Our data segment selector

movw %ax, %ds # -> DS: Data Segment

movw %ax, %es # -> ES: Extra Segment

movw %ax, %fs # -> FS

movw %ax, %gs # -> GS

movw %ax, %ss # -> SS: Stack Segment

# Set up the stack pointer and call into C. The stack region is from 0--start(0x7c00)

movl $0x0, %ebp

为何开启A20，以及如何开启A20

。在intel处理器8086中，“段：偏移”最大能表示的内存地址是FFFF：FFFF，即10FFEFh，但是8086仅仅有20位寻址地址总线，仅仅能寻址到1MB，假设试图訪问1MB以上的内存地址，并不会错误发生，而是回卷。即又回到0000:0000地址，又从零開始寻址。但是到了80286时，真的能够訪问到1MB以上的内存了。假设遇到相同的情况，系统不会再回卷寻址，这就造成了向上不兼容，为了保证100%兼容，IBM想出了一个办法。使用8042键盘控制器来控制第20个地址位。这就是A20地址线

打开A20

IN AL,0x92

OR AL,00000010b

OUT 0x92,AL

如何初始化GDT表

Gdt是全局段号记录表。将这些数据整齐地排列在内存的某个地方，然后将内存的起始地址和有效设定个数放在cpu内被称作gdtr的特殊寄存器中，设定就完成了

如何使能和进入保护