南京大学本科生实验报告

课程名称： **操作系统**

学院	计算机科学与技术		
学号	191220029	姓名	傅小龙
Email	1830970417@qq.com		

1.实验名称

Lab1:系统引导

2.实验目的

1.学习在 Linux 环境下编写、调试程序，初步掌握 Shell、 Vim、GCC、Binutils、Make、QEMU、GDB 的使用
2.学习 AT&T 汇编程序的特点
3.理解系统引导程序的含义，理解系统引导的启动过程

3.实验内容

在保护模式下加载磁盘中的 Hello World 程序并运行

实验进度描述：完成了所有内容。提交内容的项目包仅包含保护模式下加载操盘中Hello World程序的相关源码。

4. 实验过程

由于框架中已给出实模式打印Hello World，以及保护模式下打印Hello World与保护模式下加载磁盘中的Hello World程序有许多相似之处，下面仅介绍在保护模式下加载磁盘中的Hello World程序运行的实验过程

4.1 实模式到保护模式的转换

系统在启动时首先进入8086实模式，需要补充`start.s`中的代码以进入80386保护模式运行。需要关闭中断，启动A20总线，加载GDTR，设置CR0寄存器PE位为1启动保护模式，最后长跳转切换至`start32`，在保护模式下运行：

```
start:
    ...
    #TODO: Protected Mode Here
    cli # close interupt
    # start A20 main line by port 0x92
    inb $0x92
    orb $0x02, %al
    outb %al, $0x92
```

```
    data32 addr32 lgdt gdtDesc # load GDTR
    # set PE bit of $cr0 to 0x1
    movl %cr0, %eax
    orb $0x1, %al
    movl %eax, %cr0
    data32 ljmp $0x08, $start32 #long jump to protect mode
```

A20总线的启动参考了https://blog.csdn.net/chengbeng1745/article/details/82964590 给出的A20总线快速启动方式。

GDT各段描述符的设置详见 `../lab1/bootloader/start.s` 中Line93-107处相关内容，各表项的值参考课程网站给出的 `lab1.pdf` 中对保护模式的相关介绍，这里不再赘述。

4.2加载磁盘中的app程序

由 `start.s` 的 `start32` 结尾处汇编代码可知，系统切换到保护模式下后将跳转到 `boot.c` 中定义的 `bootMain()` 函数：

```
movl $0x8000, %esp # setting esp
jmp bootMain # jump to bootMain in boot.c
```

故需要向 `bootMain()` 函数中填入将 `app` 代码加载并运行的相关代码。

由 `lab1/app/Makefile` 中的内容：

```
ld -m elf_i386 -e start -Ttext 0x8c00 app.o -o app.elf
```

可知 `app.s` 生成的机器指令将被加载至 `0x8c00` 处。

故在 `bootMain()` 中创建函数指针指向 `0x8c00` 处.

根据 `lab1/Makefile` 中 `os.img` 的生成命令：

```
cat bootloader/bootloader.bin app/app.bin > os.img
```

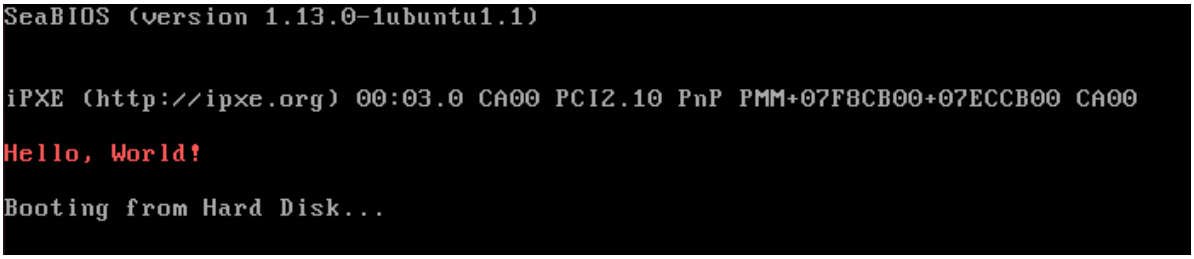
可知 `app.bin` 中内容被映射至启动分区之后，由于启动分区将占满磁盘的第0个扇区，故 `app.bin` 的内容被映射至第二个扇区. 使用 `readSect(void *dst, int offset)` 函数将磁盘1号扇区内的 `app` 的机器指令加载至该函数指针，然后调用该函数：

```
void bootMain(void) {
    void (*app)(void);
    app = (void(*)(void))0x8c00;
    readSect((void*)app, 1);
    app();
}
```

之后程序将会跳转至 `app` 中执行打印 `Hello, World!` 的相关代码。

5.实验结果

在终端中完成 `make` 后执行 `make play` 得到如下结果



6.实验总结

通过本次实验，初步了解了qemu工具的使用，加深了对操作系统引导启动过程的了解，并复习了实模式、保护模式下的操作系统的运行方式。