

Lab1

181860154 朱倩
邮箱: infinite0124@163.com

一、实验进度

完成了所有内容，提交了保护模式下加载磁盘中的Hello World程序并运行的相关源码

二、实验结果



三、实验修改的代码位置

start.s: 关闭中断，打开A20数据总线，加载GDTR，设置CR0的PE位（第0位）为1，通过长跳转设置CS进入保护模式。设置前三个GDT表项，其中代码段与数据段的基地址都为0x0，视频段的基地址为0xb8000。初始化DS，ES，FS，SS为2<<3，GS为3<<3。初始化ebp，esp，跳转到bootmain函数。

Boot.c: 在bootmain函数中定义值为Hello Word程序首地址的函数指针elf后，**增加对elf()函数的调用**，从而跳转到Hello World程序入口地址

四、思考题

GDT表项的设计

```
.word 0,0                                #GDT第一个表项必须为空
.byte 0,0,0,0

.word 0xffff,0                           #代码段描述符
.byte 0,0x9a,0xcf,0

.word 0xffff,0                           #数据段描述符
.byte 0,0x92,0xcf,0

.word 0xffff,0xb000                      #视频段描述符
.byte 0x0b,0x92,0xcf,0
```

代码段和数据段的段基址都是 0，视频段的段基址是 0xb000，三者的段限长都是 0xffff，4 位 type，DPL,S,P,AVL 等规定了各段属性，查表可得。

2020.3.3