OS Lab1 实验报告

赵思衡　201300024　zhaosh@smail.nju.edu.cn

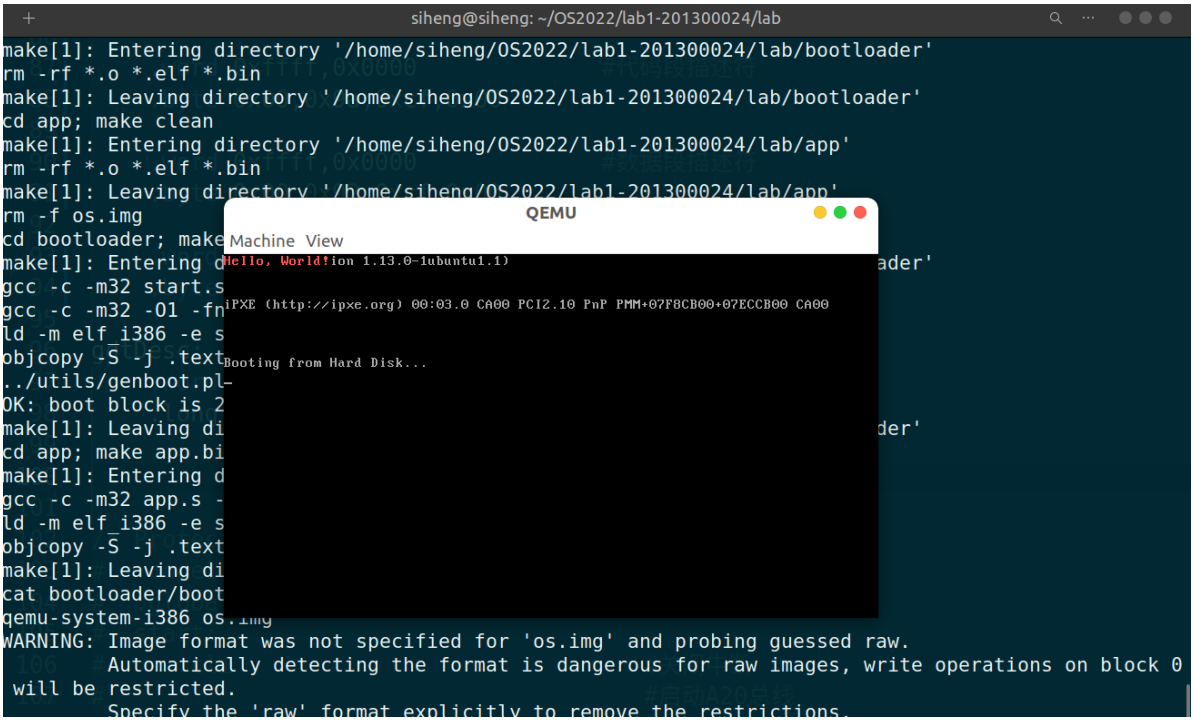
一、实验进度

我完成了所有内容。

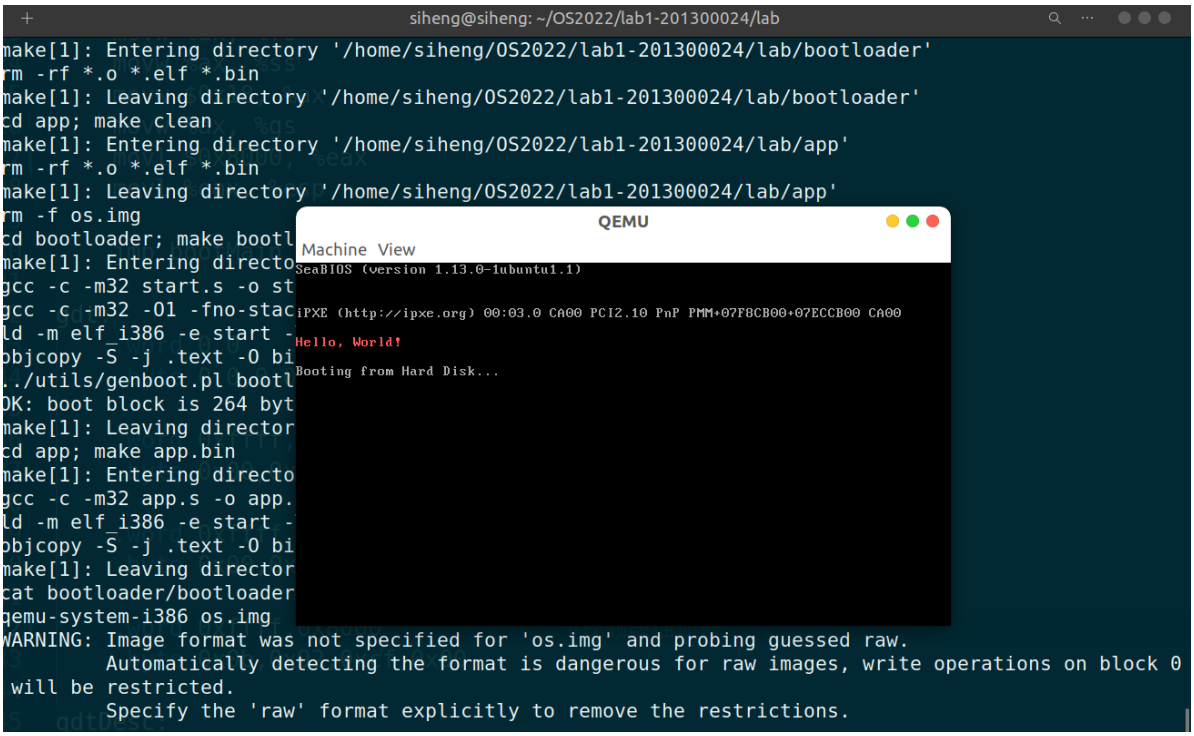
二、实验结果

Lab1.1

Lab1.2



Lab1.3



三、代码介绍

在Lab1.3中，我更改了五处代码，分别是：

1. bootloader/start.s 中 `start:` 的开启A20总线
2. bootloader/start.s 中 `start:` 的将CR0的PE位置1，开启保护模式
3. bootloader/start.s 中 `start32:` 的寄存器进行初始化
4. bootloader/start.s 中 `gdt:` 的填写GDT表内容
5. bootloader/boot.c 中 `bootMain()` 的读取OS内容并跳转执行

四、遇到的问题与想法

在填写GDT的时候，我发现通过修改ESP和视频描述段的初始地址，可以调控最终Hello World在屏幕上输出的位置，这大概是因为视频段是被映射到空间的一部分地址，通过调整段基址就可以调整最终输出的字符串在视频空间地址中的位置。

五、思考题解答

Ex1: 你弄清楚本小结标题中各种名词的含义和他们间的关系了吗？请在实验报告中阐述。

其中，CPU、内存和磁盘属于硬件，而BIOS、主引导扇区、操作系统属于软件层面。

CPU在开机后会首先启动内存中的BIOS，进行一些开机检查，之后会由BIOS将磁盘的主引导扇区加载如内存，之后会由主引导扇区将操作系统加载进内存完成接下来的工作。

Ex2: 中断向量表是什么？你还记得吗？请查阅相关资料，并在报告上说明。

中断向量表是一种硬件识别中断的方式，在这种方式下，异常或中断处理程序的首地址称为中断向量，所有中断向量存放在一个表中，称为中断向量表。每个异常或中断都被设定一个中断类型号，中断向量存放的位置与对应的中断类型号有关。

Ex3: 为什么段的大小最大为64KB，请在报告上说明原因。

因为在实模式下，数据线和寄存器均是十六位，若想表示段内偏移地址，最多为$2^{16} = 64$KB。

Ex4: genboot.pl其实是一个脚本程序，虽然我们没学过这种脚本语言，但可以大概看出来，它先打开mbr.bin，然后检查文件是否大于510字节等等。请观察genboot.pl，说明它在检查文件是否大于510字节之后做了什么，并解释它为什么这么做。在实验报告中简述一下。

```
$buf .= "\0" x (510-$n);
```

一句表示将文件后的字节全部置0直到第510字节

```
$buf .= "\x55\xAA";
```

一句表示将第511和512字节置为魔数，以便后续检查

Ex5: 请简述电脑从加电开始，到OS开始执行为止，计算机是如何运行的。简略描述即可。

从电脑开始加点时，第一条指令是跳转到BIOS固件开始执行，进行启动的一些基本检查，之后BIOS会将磁盘的主引导扇区的MBR加载到内存的`0x7c00`处，由MBR从实模式切换到保护模式，建立GDT表等内容，之后再由MBR加载OS进行操作。