Lab1 实验报告

PB21000033 赵奕

一、实验目标

- 以 multiboot 为启动协议，qemu 作为 bootloader 启动一个小型 os 内核
- 测试 qemu 对串口的支持

二、实验原理

multiboot 启动协议指定了引导加载程序和操作系统之间的接口，使任何兼容的引导加载程序都应该能够加载任何兼容的操作系统。该规范并未指定引导加载程序应如何工作——仅指定它们必须如何与正在加载的操作系统交互。该规范主要针对 PC，且主要支持 32 位系统 (但不是一定的)

qemu 是一套模拟处理器软件，在 GNU/Linux 平台上使用广泛，常用于模拟操作系统运行，在本实验中用以测试我们的 multiboot 启动

grub 是一个来自 GNU 项目的多操作系统启动程序。允许用户可以在计算机内同时拥有多个操作系统，并在计算机启动时选择希望运行的操作系统。在本实验中使用 grub 来启动了运行在 qemu 上的我们的小型操作系统内核

VGA 视频图形阵列是 IBM 于 1987 年提出的一个使用模拟信号的电脑显示标准，是显卡上应用最为广泛的接口类型，传输红、绿、蓝模拟信号以及同步信号 (水平和垂直信号)。本实验中我们基于 VGA 协议将信息输出到了 qemu 界面中。

串口输出是 qemu 提供的一种输出信号的方式。在运行时使用的`-serial stdio` 指定串行终端为标准输入输出，使我们最终可以在终端看到串口输出的信号内容。

三、源代码说明

实验文件包括: Makefile 文件, .ld 和.S 文件。

Makefile 作用为使.S 文件编译生成.o 并最终链接生成.bin 文件。
.ld 文件是链接文件, 写了代码格式和代码排布内存布局
.S 文件里面存放汇编代码。其中头部留出 12 个字节 (以及 4 个字节的冗余)，每个 VGA 输出的字符两个字节，将每个字符连续存放于一片地址空间中得到最后结果。并使用了串口输出 (使用寄存器) 输出到 stdio 中

VGA 输出

VGA 输出从地址 0xB8000 开始。
`movl $0x096f093c, 0xb8000` 表示输出底色为黑色,字色为深蓝的两个字符 0x6f, 0x3c (对应 <o) 到最开始的两个位置。
之后的输出，地址逐次 +4

串口输出

stdio 对应的串口编号是 $0x3F8，用 movw $0x3F8，%dx 存到 %dx 寄存器中。
接下来 movb $0x7a，%al 将 0x7a(即 z）存到 $al 寄存器中，并用 outb %al，%dx 将寄存器中的内容输出到串口。

四、代码布局说明

从物理内存 1M 开始放置内容代码。
一开始的 12 个字节存放了一些信息 (MAGIC, FLAGS, CHECKSUM)

在 .ld 文件中定义的 . = ALIGN(8); 表示在此之后按照每 8 字节对齐
从 1M+16 字节开始放置代码

每个输出到屏幕的字符需要 2 个字节（一个字节的颜色，一个字节的内容），每条 movl 指令对应 2 个字符，所以相当于对应了 4 个字节的内容，因此 movl 指令中间目标地址相差为 4

五、编译过程说明

生成 .bin 文件使用命令

```
make
```

实际上运行了两个指令

```
gcc -c ${ASM_FLAGS} multibootHeader.S -o multibootHeader.o
ld -n -T multibootHeader.ld multibootHeader.o -o multibootHeader.bin
```

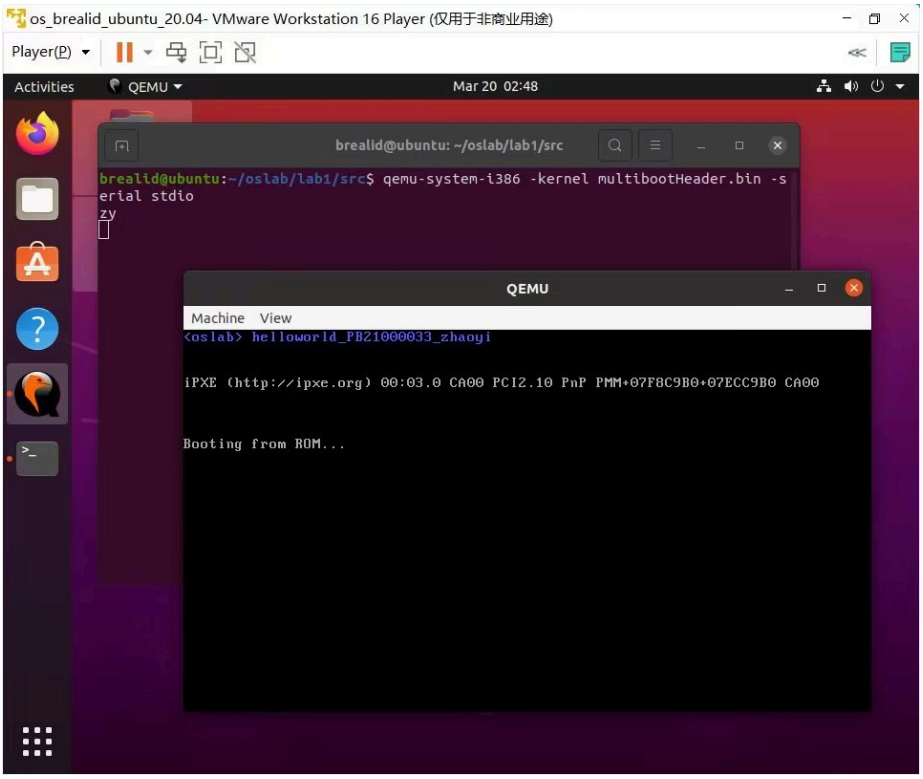
第一句用以编译.s 文件并生成.o 文件，第二句将.o 文件和.ld 文件链接起来生成.bin 文件
其中 ${ASM_FLAGS} 是 -m32 --pipe -Wall -fasm -g -O1 -fno-stack-protector，为一些编译参数。

运行 qemu 使用命令

```
qemu-system-i386 -kernel multibootHeader.bin -serial stdio
```

其中，- qemu-system-i386 指定平台为 i386 - -kernel 指定内核文件 - -serial stdio 指定串行终端为标准输入输出

六、实验结果



七、遇到的问题和解决方法

1. 安装完 qemu 之后，qemu-system-i386 无法运行。需要使用 apt install qemu-system-i386 以安装特定版本的 qemu

2. 运行 qemu 出现 Error loading uncompressed kernel without PVH ELH Note。解决方案：在 .section(header) 处添加 .align 4