Report for Lab3——实模式下的Hello World

Stu：金泽文

No.PB15111604

实验内容：

1. 编写一段16进制的汇编程序，用作启动扇区代码
2. 编写一个链接脚本，将启动代码按照启动扇区进行链接
3. 制作启动软盘，将启动扇区代码安装到软盘的启动扇区(也可以选择其他介质)
4. 启动运行启动扇区代码，最后进入死循环
5. 编写一个shell脚本文件，将make，制作启动软盘，启动运行等步骤放在这个脚本文件中

实验步骤：

·学习x86汇编，并编写一段16进制的汇编程序，用作启动扇区代码。

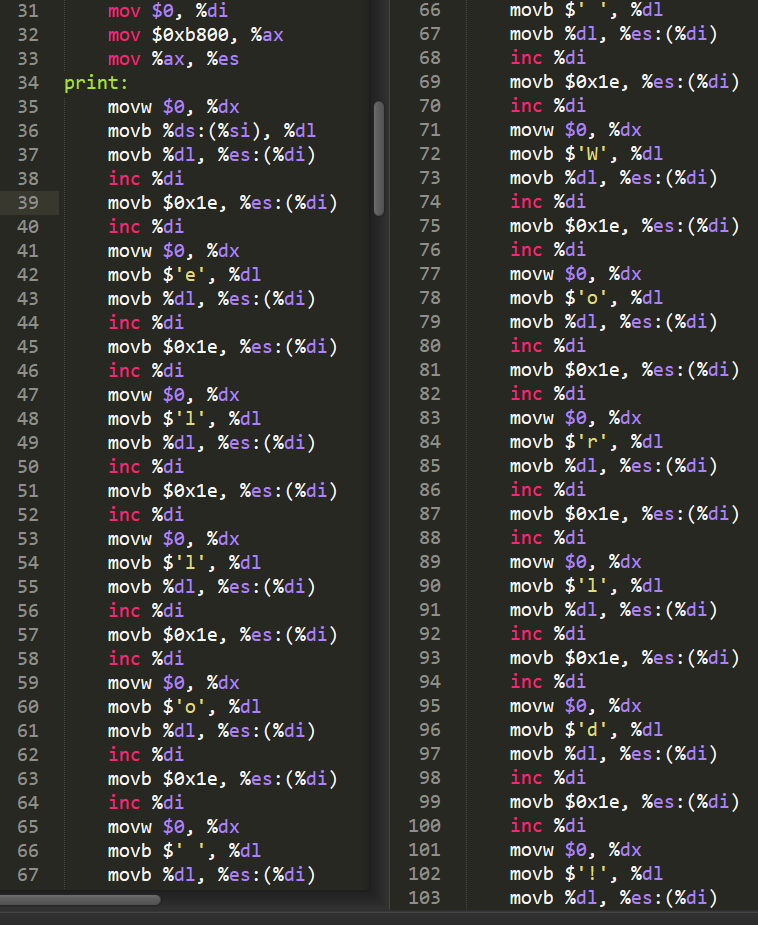
参考 [这篇博客](http://www.cnblogs.com/orlion/p/5765339.html)，以及《Computer System: A Programer’s Perspective》学习简单的x86汇编（AT&T格式）。

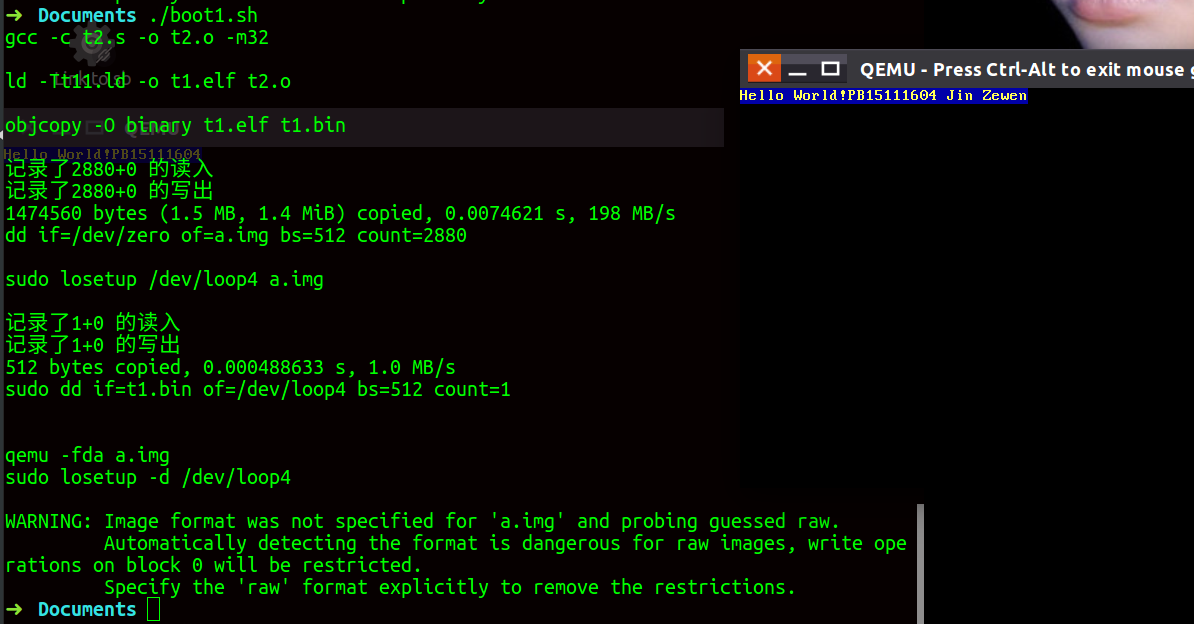
·学习并编写一个链接脚本，将启动代码按照启动扇区进行链接。

参考[这个博客](http://blog.csdn.net/mrwangwang/article/details/9097411)（写完意外地发现老师在群里发了一个ld脚本，嘤嘤嘤）

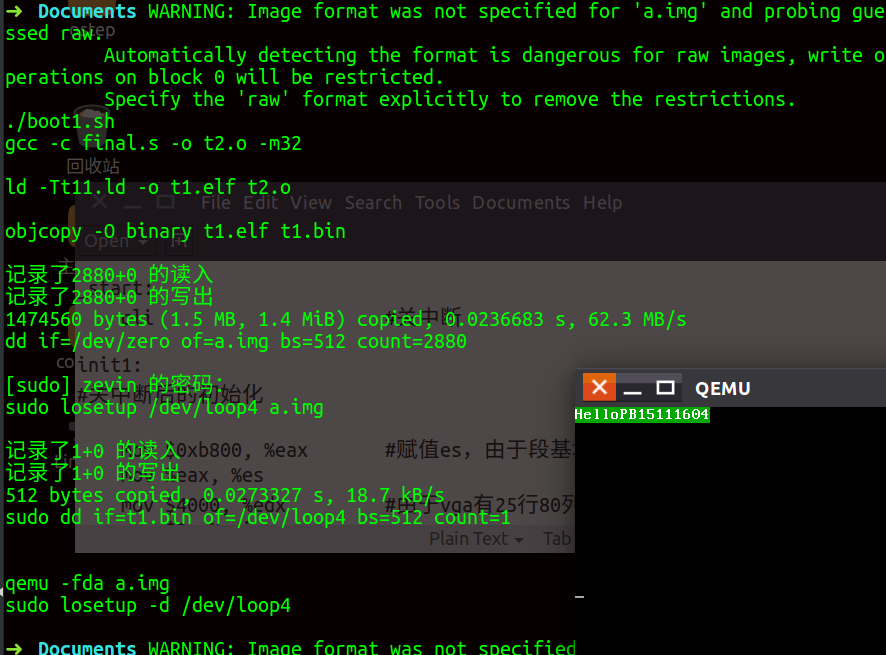
·同时，为了方便之后n次的反复操作，编写了整个shell脚本。

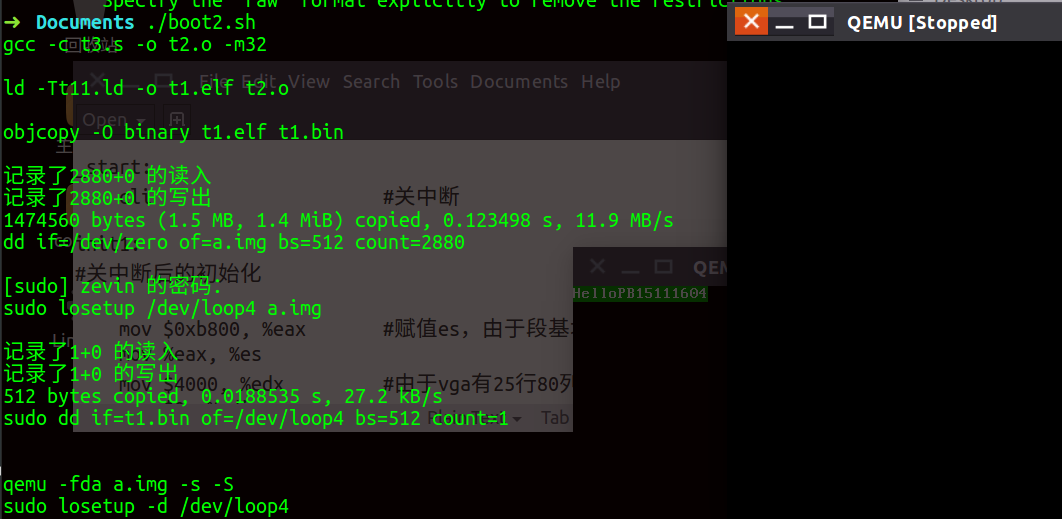
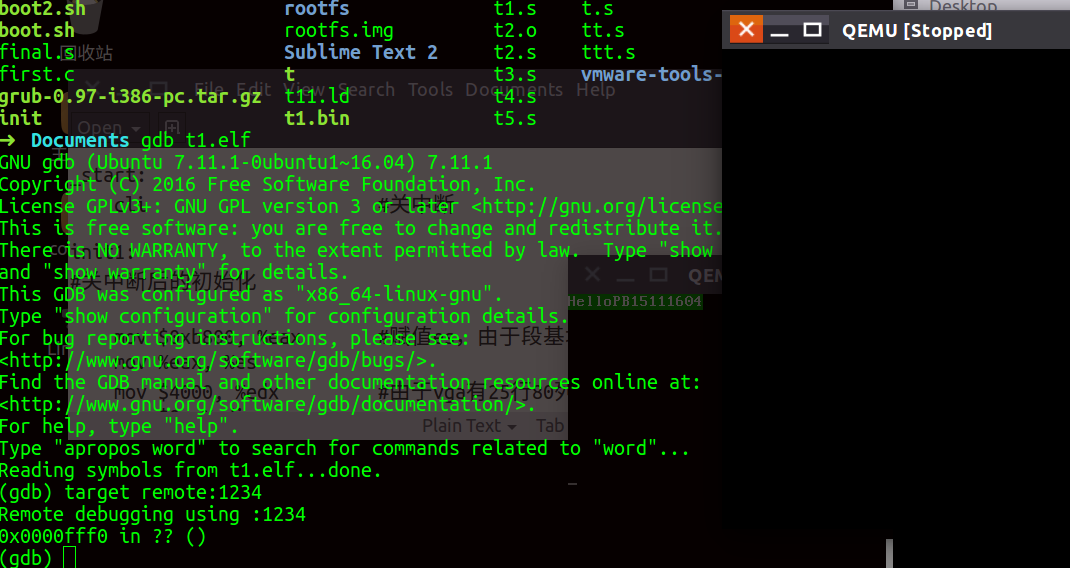
刚开始的时候，不知道有lodsb，movsb等routine，所以暴力存取，并且当时理解错了data section text section的用法，没能正确读取字符串的地址，所以只好手动将字符存入到vga中。当时的代码是这样的。



在听送小牛说有movsb这种好东西并且调试n次之后，得到以下结果。（当时要求的明明是输出这个东西“hello world pb15111604 jinzewen”。产品经理竟然改需求。）

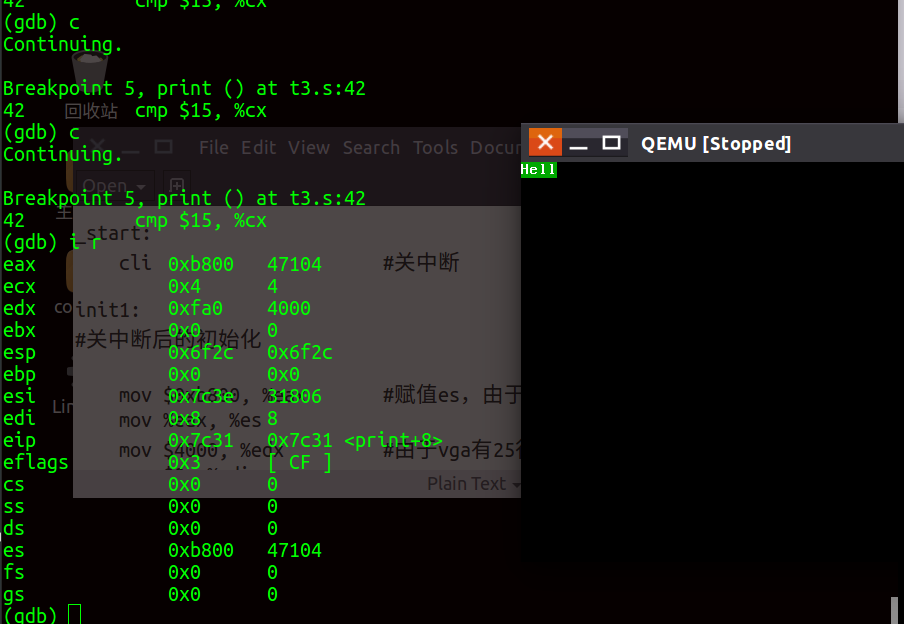
之后更改得到如下图所示。



以下是调试过程的截图：

清屏之后



Print中间查看寄存器

实验步骤部分结束。

回答问题：

1. 什么是BIOS？BIOS和启动软盘之间的启动协议是什么？

软盘的启动扇区最后两字节如果是0xaa55，那么软盘即为启动设备，否则识别软盘为unbootable device。

1. 启动时为什么要关中断

关中断 ，能够避免在启动时被意料之外的中断所干扰。保证启动过程安全进行。同时，不让我们用中断写入到vga中，而是自己直接写入显存。

1. 什么是实模式？实模式初始化哪些寄存器？

实模式就是在位宽只有16位的情况下实现20位的寻址空间（即1MB）。实模式通过段：段内偏移来实现20位。需要初始化cs、ds、ss、si、di等寄存器。

1. VGA的接口是什么，如何编程实现VGA输出

Vga的接口即为vga显存地址内容。（或者说没有接口，直接存取？）实模式下，由于vga显存从0xb8000开始，每个字符对应两个字节，分别存放属性和字符，所以只要对应赋值即可。

1. 什么是链接脚本？启动软盘的链接脚本有哪些注意的地方？

链接脚本用于规定如何把输入文件的section对应地放入到输出文件中，并控制输出文件各部分在内存空间中的布局。启动软盘的OUTPUT\_FORMAT应该对应我们操作系统下正确的elf格式，即elf32-i386，OUTPUT\_ARCH对应正确的i386，并且ENTRY要对应正确的汇编代码中的global起始常量，在我的汇编代码中对应的是\_start部分。由于软盘空间从0x7c00开始，所以要把输出文件起始地址对应到内存空间的0x7c00处。另外，为了最后两个0xaa55，可以设置.signature。（也可以不在这里设置，而直接在汇编代码中设置。）

1. 从Power-on开始，说清楚计算机是如何一步一步启动，直到开始运行你写的代码

①BIOS

从通电开始，ROM内的BIOS程序被读取并执行。BIOS先检查硬件是否满足启动条件。硬件自检之后，开始按照启动顺序依次访问各个设备对应的MBR，如果最后两个字节为0xaa55，则认定为启动程序，否则继续检查。

②MBR

正常情况下，MBR包含操作系统的调用信息，以便计算机继续启动。MBR还包括分区表，以及最后两个上面提到的0xaa55。

而在我们这次实验中，我们的汇编代码转化的二进制代码直接存放在了启动软盘上面，所以直接被计算机所执行。

1. 给出代码运行关键时刻的截屏并加以说明。

这一步在最前面都有详细的交代。

【感谢】感谢积极回答我的问题并丝毫没有嫌弃我的陈香兰老师，以及与跟我一起积极讨论并给予帮助的宋小牛同学。

参考

【1】http://www.cnblogs.com/orlion/p/5765339.html

【2】http://blog.csdn.net/mrwangwang/article/details/9097411