

软件综合实验之操作系统

加载操作系统映像并进入C

陈香兰

中国科学技术大学计算机学院

July 1, 2016

- 1 实验准备
- 2 加载操作系统映像并进入C
- 3 小结

- 实验环境准备

- 编译工具链：gcc、ld
- 代码维护工具：make
- 模拟环境：qemu-system-i386

- 基础知识准备

- 软盘相关BIOS中断：从软盘上读取操作系统映像
- 准备执行C语言代码

从软盘上读取操作系统映像 I

- 软盘相关BIOS中断：int 0x13

https://en.wikipedia.org/wiki/INT_13h#INT_13h_AH.3D00h:_Reset_Disk_Drive

- Drive Table

DL	Description
00h	1st floppy disk (“drive A:”)
01h	2nd floppy disk (“drive B:”)
80h	1st hard disk
81h	2nd hard disk

- Function Table

AH	Description
00h	Reset Disk Drives
02h	Read Sectors From Drive

- ① INT 13h AH=00h: Reset Disk Drive

AH	00h
DL	Drive

② INT 13h AH=02h: Read Sectors From Drive

AH	02h
AL	Sectors To Read Count
CH	Cylinder[7:0]
CL	Cylinder[9:8]:Sector[5:0]
DH	Head
DL	Drive
ES:BX	Buffer Address Pointer

- 思考：何时加载操作系统映像合适？加载多少个扇区合适？

准备执行C语言代码

- 为执行C语言代码准备好栈
 - 什么位置合适？
- 将BSS段清0
 - 什么是BSS段？

- 参见GNU开发工具链简介中关于make的部分

加载操作系统映像并进入C

① 阅读源代码

- start16.S
- start16.ld
- start32.S
- main.c
- myOS.ld
- Makefile

② 编译链接并制作成二进制映像

- make

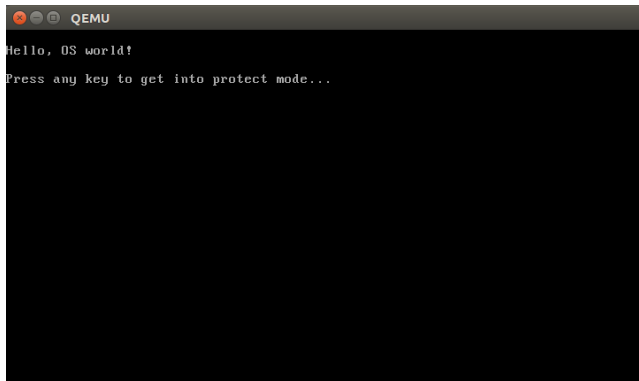
③ 制作启动软盘

- `dd if=/dev/zero of=a_boot2C.img bs=512 count=2880`
- `sudo losetup /dev/loop4 a_boot2C.img`
- `sudo dd if=start16.bin of=/dev/loop4 bs=512 count=1`
- `sudo dd if=output/myOS.bin of=/dev/loop4 bs=512 seek=1`

加载操作系统映像并进入C

在qemu上启动

- `qemu-system-i386 -fa a_boot2C.img`

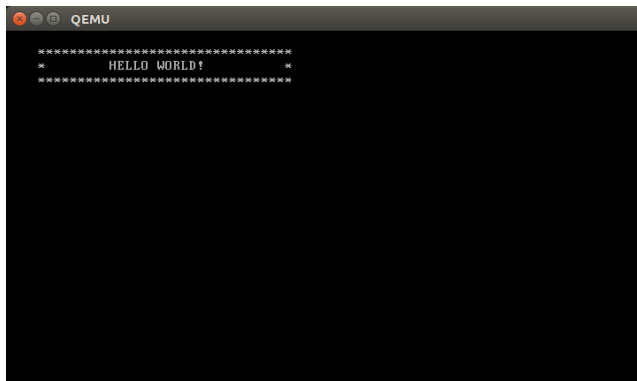


```
QEMU
Hello, OS world!
Press any key to get into protect mode...
```

加载操作系统映像并进入C

在qemu上启动

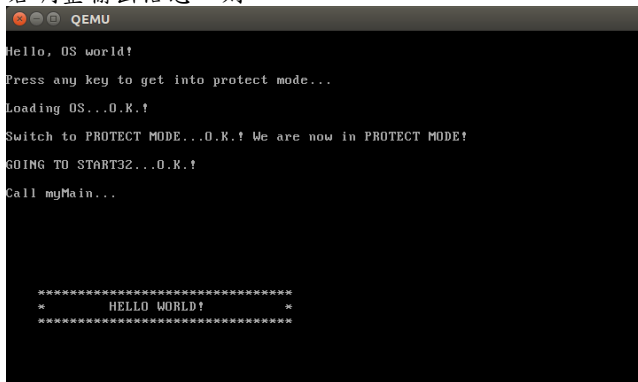
- `qemu-system-i386 -fa a_boot2C.img`



加载操作系统映像并进入C

在qemu上启动

- `qemu-system-i386 -fa a_boot2C.img`
- 若调整输出信息，则



```
QEMU
Hello, OS world!
Press any key to get into protect mode...
Loading OS...O.K.!
Switch to PROTECT MODE...O.K.! We are now in PROTECT MODE!
GOING TO START32...O.K.!
Call myMain...

*****
*          HELLO WORLD!          *
*****
```

- 查看bin文件
 - `hexdump -C output/start16.bin`
 - `hexdump -C output/myOS.bin`
- 查看img文件
 - `hexdump -C output/a_boot2C.img`

谢谢！