

**实验报告**



**题目： 键盘驱动程序的分析与修改**

**班 级： 2022211313**

**学 号： 2022211363**

**姓 名： 谢牧航**

**学 院： 计算机学院**

**2022年 11 月 日**

一、实验目的  
1.理解I/O系统调用函数和C标准I/O函数的概念和区别；

2.建立内核空间I/O软件层次结构概念，即与设备无关的操作系统软件、设备驱动程序和中断服务程序；

3.了解Linux-0.11字符设备驱动程序及功能，初步理解控制台终端程序的工作原理；

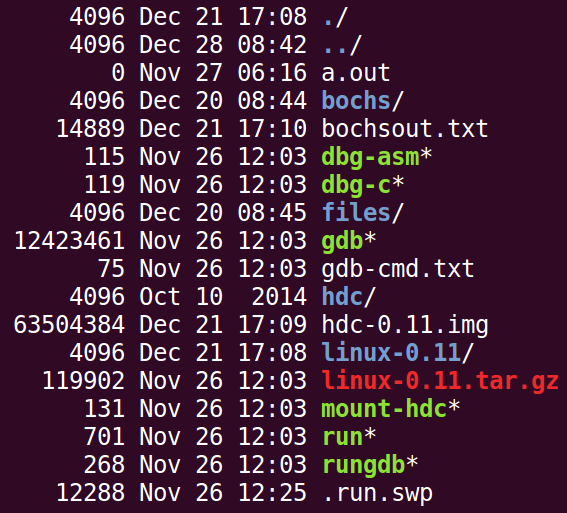
4.通过阅读源代码，进一步提高C语言和汇编程序的编程技巧以及源代码分析能力；

5.锻炼和提高对复杂工程问题进行分析的能力，并根据需求进行设计和实现的能力。

1. 实验环境
2. 硬件：学生个人电脑（x86-64）
3. 软件：Windows 10，VMware Workstation 15 Player，32位Linux-Ubuntu 16.04.1
4. gcc-3.4编译环境
5. GDB调试工具

三、实验内容

从网盘下载lab4.tar.gz文件，解压后进入lba4目录得到如下文件和目录：



实验常用执行命令如下：

* 执行./run ，可启动bochs模拟器，进而加载执行Linux-0.11目录下的Image文件启动linux-0.11操作系统
* 进入lab4/linux-0.11目录，执行make编译生成Image文件，每次重新编译（make）前需先执行make clean
* 如果对linux-0.11目录下的某些源文件进行了修改，执行./run init 可把修改文件回复初始状态

本实验包含2关，要求如下：

* Phase 1

键入F12，激活\*功能，键入学生本人姓名拼音，首尾字母等显示\*

比如：zhangsan，显示为：\*ha\*gsa\*

* Phase 2

键入“学生本人学号” ：激活\*功能，键入学生本人姓名拼音，首尾字母等显示\*

比如：zhangsan，显示为：\*ha\*gsa\*，

再次键入“学生本人学号-” ：取消显示\*功能

提示：完成本实验需要对lab4/linux-0.11/kernel/chr\_drv/目录下的keyboard.s、console.c和tty\_io.c源文件进行分析，理解按下按键到回显到显示频上程序的执行过程，然后对涉及到的数据结构进行分析，完成对前两个源程序的修改。修改方案有两种：

* 在C语言源程序层面进行修改
* 在汇编语言源程序层面进行修改

实验4的其他说明见lab4.pdf课件和爱课堂中虚拟机环境搭建相关内容。linux内核完全注释(高清版).pdf一书中对源代码有详细的说明和注释。

四、源代码的分析及修改

针对一次按键操作对源代码keyboard.s、console.c和tty\_io.c的进行分析，说明分析过程，要配有流程图（不能从书中进行截图）进行说明，给出各阶段的修改思路和代码实现。各阶段需要有较详细的文字说、运行截图、分析过程的内容。

## Phase 1

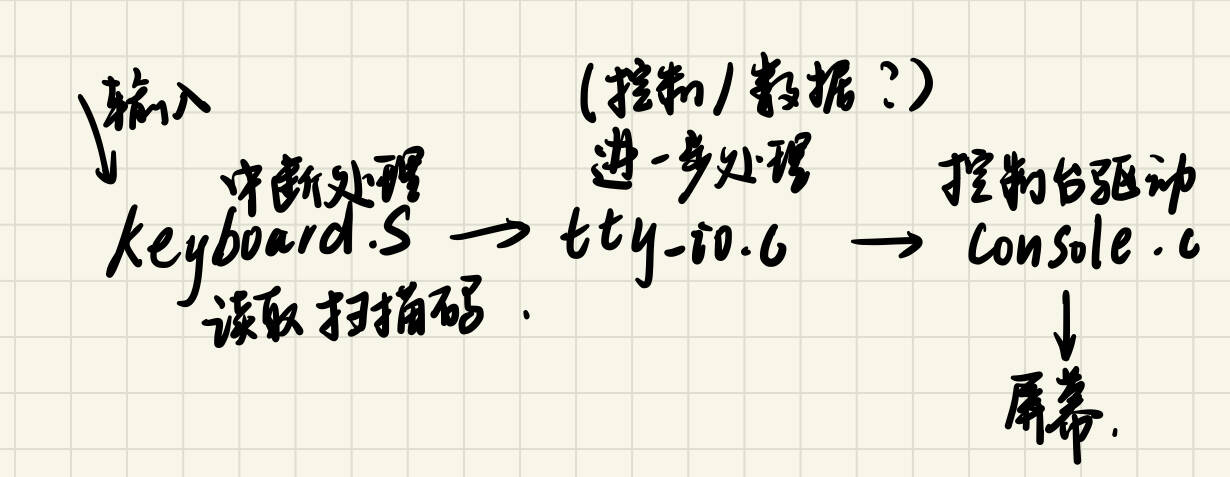
要理解 Linux 内核的特定部分，首先需要深入研究《Linux 内核完全注释》，特别是 Linux 0.11 版本内核中位于 linux-0.11/kernel/chr\_drv/ 目录下的三个关键文件：keyboard.S、console.c 和 tty\_io.c。这些文件分别承担着不同的核心功能：

1. keyboard.S：这是一个键盘中断处理程序。它的主要职责是处理用户敲击键盘时产生的字符输入。在这个程序中，每次键盘活动都会触发中断，该程序随后对这些中断做出响应。

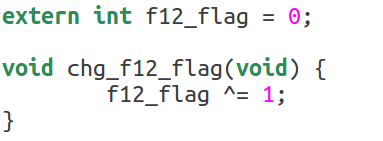
2. console.c：这个文件负责显示控制。它实现了控制台终端的输出处理，意味着当代码产生输出时，它决定了这些输出如何在用户屏幕上显示。

3. tty\_io.c: 控制缓冲队列的程序。

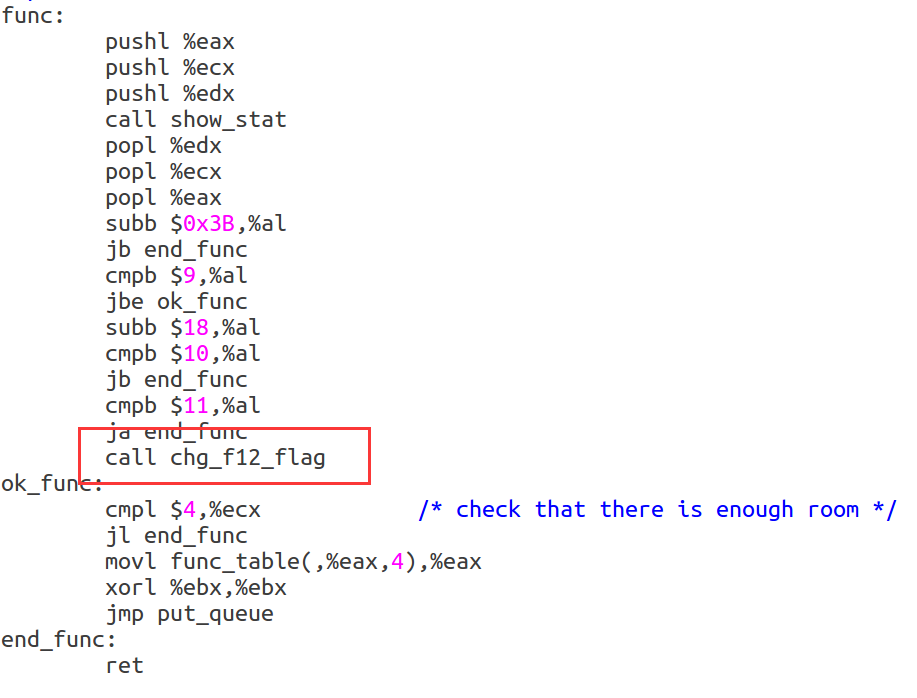
流程图如下：



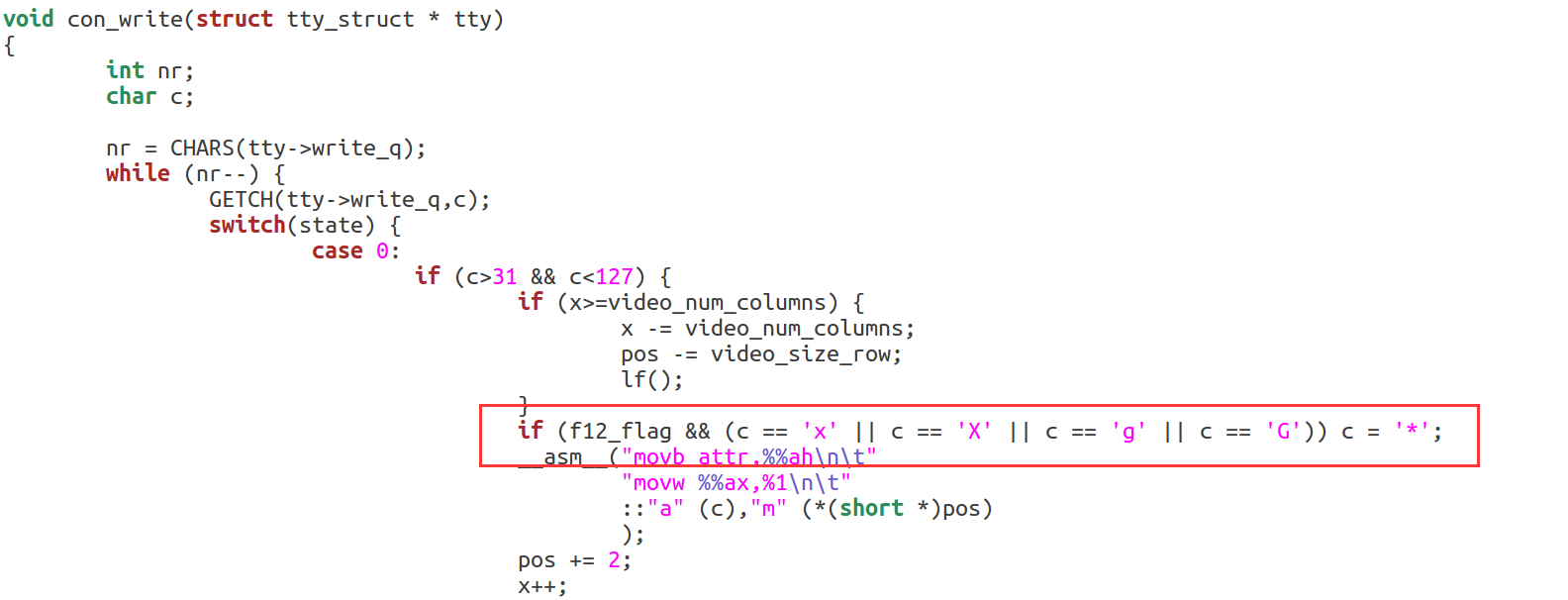
对于console.c，阅读书籍种的注释发现con\_write是控制台写函数，其中char c即本次读进来的字符。我们需要在F12状态下使x和g字符变为星\*，再点一下恢复。所以我们可以写下面这个chg\_f12\_flag函数。每次点击F12后Flag的状态翻转。

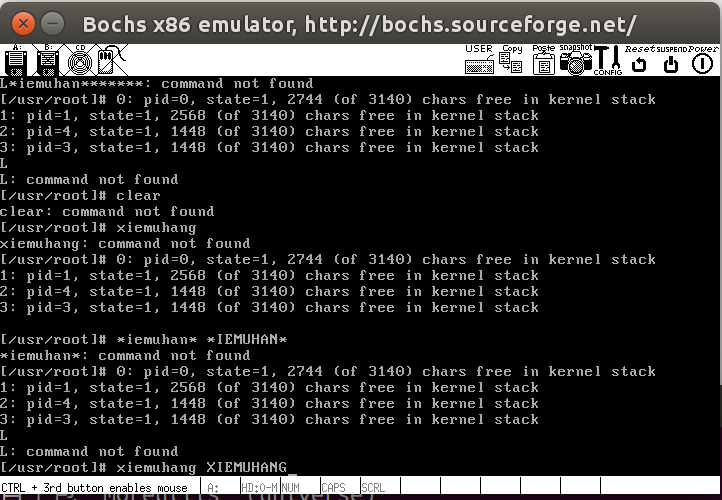


对于keyboard.S文件，我们发现fun函数部分是处理F1~F12功能键的，阅读注释后我们在这个地方设置调用chg\_f12\_flag函数即可。这样每次点击F12都会调用chg\_f12\_flag函数。



接下来修改con\_write函数，我们在flag为1的时候把x和g字符替换为\*即可。

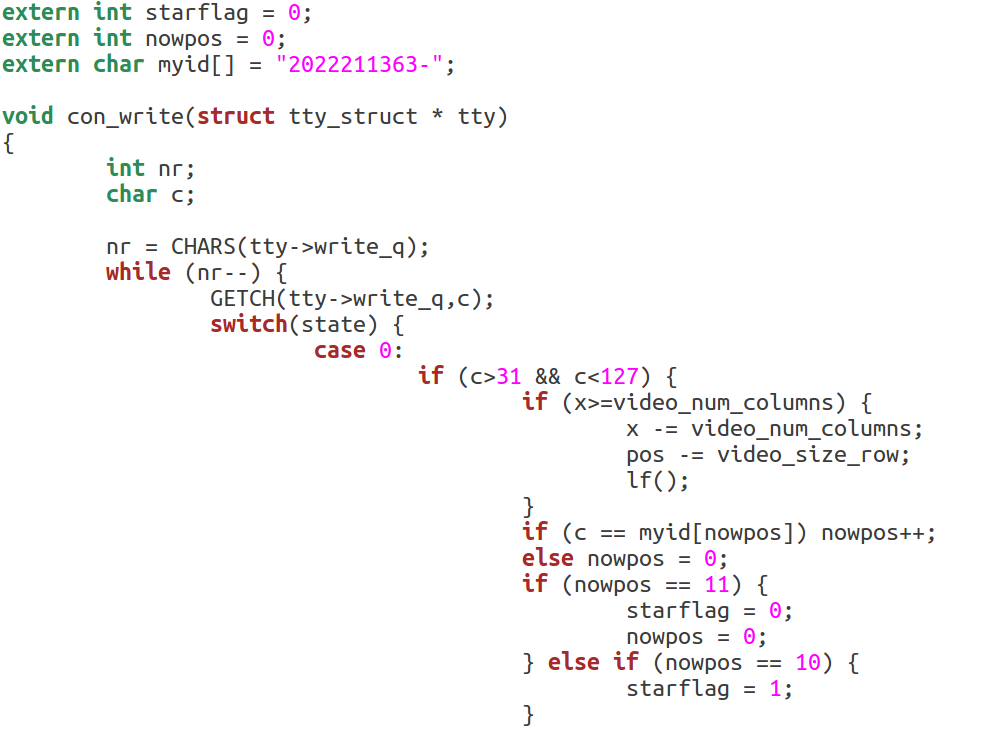




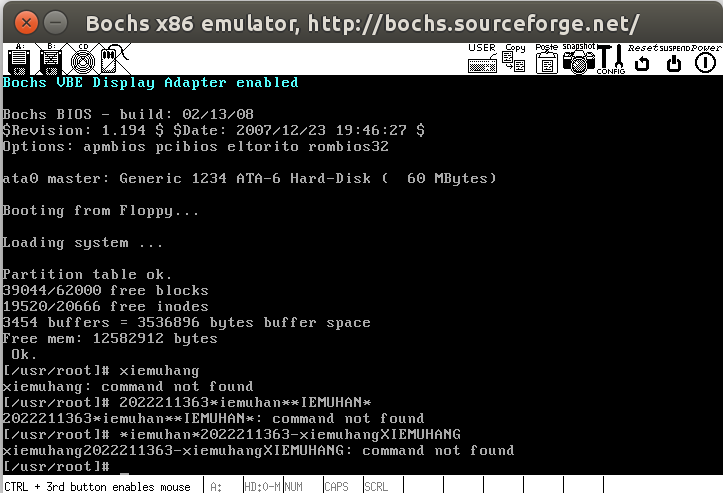
重新编译内核并运行，运行结果如上。点击F12后，x和g字符替换为\*，再点一次恢复。

## Phase 2

在Phase 1的启发下我们只需要修改console.c文件即可。当我们连续读入2022211363时，打开星号模式，若连续读入2022211363-，则退出星号模式。编写代码如下：



如果输入字符连续和myid相同到第9位，那么nowpos变为10，此时打开星号模式，如果继续相同到第10位，那么nowpos变为11，退出星号模式。其他情况下都不会影响输入。



重新编译内核并运行，运行结果如上。输入2022211363打开星号模式，输入2022211363-关闭星号模式。

五、总结体会

总结心得（包括实验过程中遇到的问题、如何解决的、过关或挫败的感受、实验投入的时间和精力、意见和建议等）

通过这次实验，我对Linux中的I/O有了更深入的了解，特别是通过《Linux内核完全注释》来理解键盘驱动程序的工作原理，并且我还实现了修改Linux内核中的键盘驱动程序，以改变Linux控制台中的字符回显。

总的来说，这次实验则让我更加深入地理解了Linux操作系统及其I/O处理机制，为之后深入学习Linux系统打下了基础。