[2][1][3]

西南林业大学

本科毕业（设计）论文

(二〇一八届)

题　　目： RongOS — 一个简单操作系统的实现

分院系部： 计算机与信息科学学院

专　　业： 计算机科学与技术专业

姓　　名： 蒲启元

导师姓名： 王晓林

导师职称： 讲师

二〇一八 年 六 月

RongOS — 一个简单操作系统的实现

蒲启元

（西南林业大学 计算机与信息科学学院，云南 昆明 650224）

摘　要： 操作系统管理着计算机的硬件和软件资源，它是向上层应用软件提供服务（接口）的核心系统软件，这些服务包括进程管理，内存管理，文件系统，网络通信，安全机制等。操作系统的设计与实现则是软件工业的基础。为此，在国务院提出的《中国制造 2025》中专门强调了操作系统的开发。但长期以来，操作系统核心开发技术都掌握在外国人手中，技术受制，对于我们的软件工业来说很不利。本文从零开始设计开发一个简单的操作系统，包括 boot loader，中断，内存管理，图形接口，多任务，以及在这个系统上的几个小应用等。尽管这个系统很简单，但它为自主开发操作系统做了一个小小的尝试。

关键词： 操作系统，进程，内存，中断，boot loader

RongOS — A simple OS implementation

Qiyuan Pu

School of Computer and Information Science
Southwest Forestry University
Kunming 650224, Yunnan, China

Abstract: Operating system manages the sources of hardware, it lies in the core of the system software and provides services(interfaces) to upper applications. These service including process management, memory management, file system, network communication, security mechanism etc. Operating system development is the foundation and core of software industry. Therefore, «Made in China 2025» emphasize the development of operating system that put forward by The State Council of China. For a long time, however, the OS kernel development technology grasped in the hand of foreigner, it's bad for our software industry cause of limited technology. So this article will design and develop a simple operating system, including boot loader, interrupt, memory management, graphic interface, multitasking, and some little applications based on this system. In spite of the simplicity of this system, it's a small trying for autonomous development operating system.

Key words: operating system, boot loader, process, interrupt, memory management

目　录

插图目录

表格目录

1 Introduction

1.1 Background

1.2 Preliminary Works

1.2.1 Development Environment

Operating System: Debian 4.11.0-1-amd64

Debug System: QEMU emulator version 2.8.1(Debian 1:2.8+dfsg-7)

Emacs version: GNU Emacs 25.2.2

1.2.2 Tools

Some tools used to develop RongOS, see tools.[1].

1.2.3 Install

Debian System: there is a small tutorial.[2]

QEMU, for my x86_64 architecture:

```
$ sudo apt-get install qemu-system-x86_64
```

Note that the tools is exe formate, so on Debian system, you need to install wine:

```
$ sudo apt-get update
$ sudo apt-get install wine
```

Maybe you also need to add i386 architecture cause of AMD64 on your machine to use these tools:

```
$ sudo dpkg --add-architecture i386
```

[1] https://github.com/Puqiyuan/RongOS/tree/master/Tools
[2] http://cs2.swfc.edu.cn/~wx672/lecture_notes/linux/install.html

```
$ sudo apt-get update
```

2 Design

2.1 Top Level Design

2.2 Detailed Design

2.2.1 Boot Loader

This is working flow of boot loader:

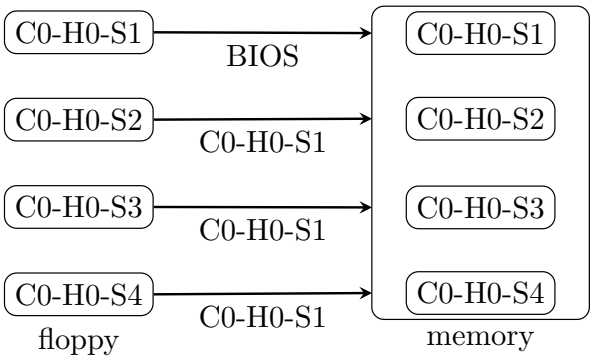

图 2-1 Working Flow of Boot Loader

The instructions of boot loader saved in C0-H0-S1 of floppy, the first cylinder, head 0, the first sector, total 512 byte. These instructions end with 0x55 0xaa, so BIOS will load C0-H0-S1 to memory, then the instructions in C0-H0-S1 will load C0-H0-S2 — C9-H1-S18, total $10 * 2 * 18 * 512 = 184320byte = 180KB$(including boot sector, C0-H0-S1) to main memory.

2.2.2 32-bit Mode and Import C Codes

3 Implementation

3.1 Boot Loader

3.1.1 Chose Disk

There are many ways to boot a operating system, from hard disk, USB, floppy disk etc. I chose floppy disk, although it is out of date. For my purpose is that develop a simple operating system, pay my attention on how to development. The structure of floppy disk is simple and for my simple operating system it's enough.

3.1.2 The Structure of Floppy Disk

This picture show the inside of floppy disk:

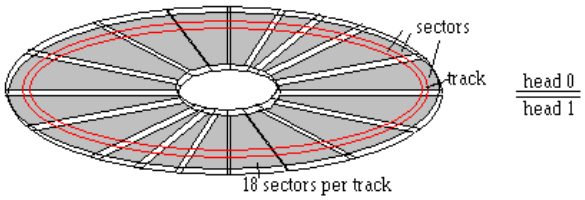

图 3-1 Floppy Disk Structure

The floppy store information in two sides. There are 80 cylinders from the outermost to the core in each side, numbering 0, 1, ..., 79. The head can assign be 0 or 1, representing two sides of floppy. When specify head number and cylinder number, forming a ring, named track in jargon. The track is large so we divide it to 18 small parts, named sector. A sector can store 512 byte. So the capacity of a floppy is:

$$18 * 80 * 2 * 512 = 1474560Byte = 1440KB.$$

The IPL(Initial Program Loader) in C0-H0-S1(cylinder 0, head 0, sector 2), and the next sector is C0-H0-S2.

3.1.3 Flowchart of Boot Loader

The following is the flowchart of boot loader:

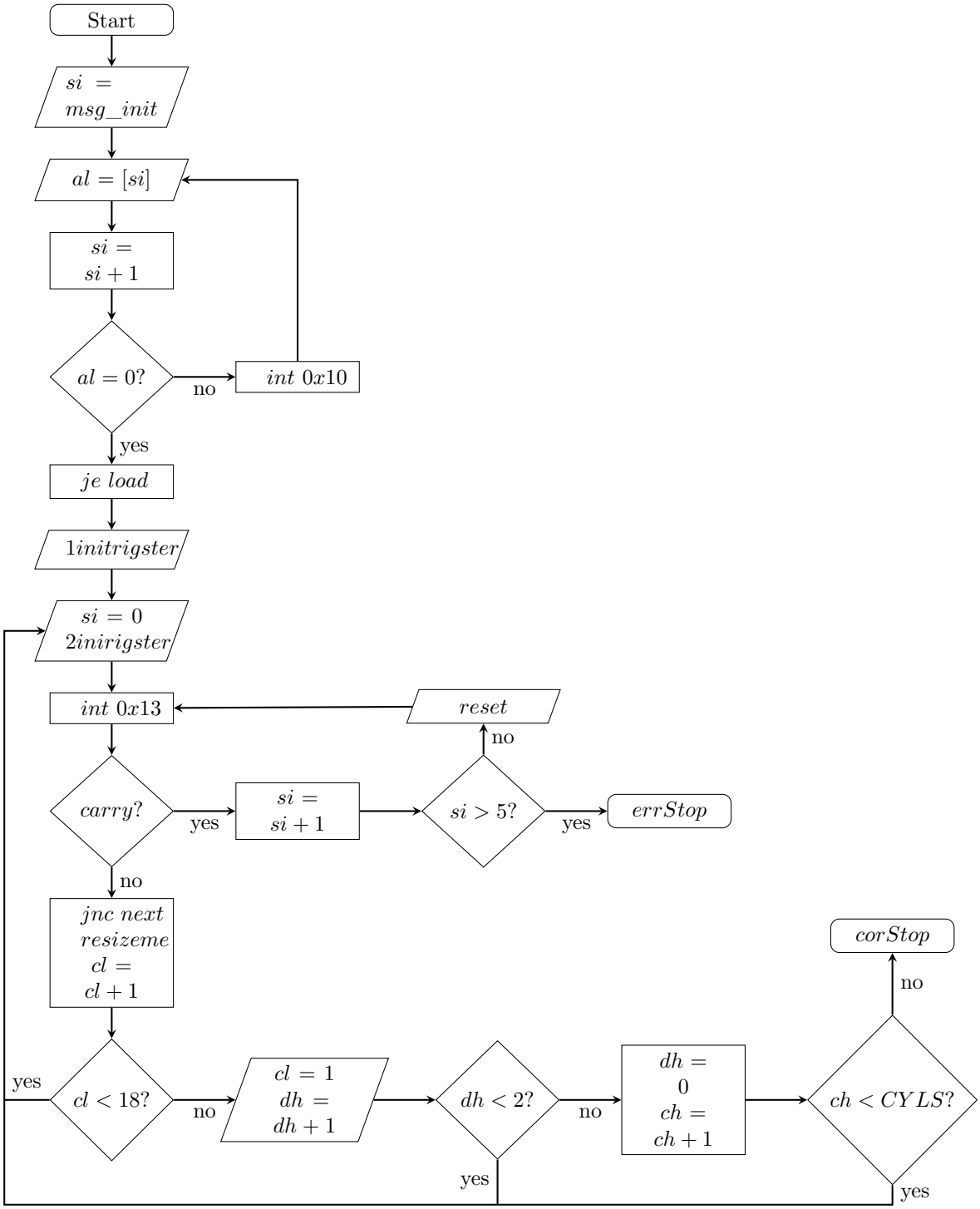

图 3-2 Flowchart of Boot Loader

Firstly, the boot sector display some boot information, when $al = 0$, the null character of boot information hit. Interrupt $0x10$ is used for show a character.

Then jump to load C0-H0-S2, ax register saved the address where beginning puts the sectors from floppy. And preparing parameters for interrupt $0x13$ in registers. The $0x13$ interrupt used for read sector from floppy to memory.

If there is a carry, representing some thing wrong when read floppy, so reset the registers and try again read floppy, until five times trying. Register si is a counter. If no carry, jump to next segmentation, as one sector read to memory already, the address space should increase 512 byte. Then sector number(cl register) added 1 and compare it to 18, if it's smaller than 18, jump to $readloop$, read the next sector. If the value of cl register bigger or equal to than 18, meaning that one track 18 sector in this side of floppy read already, then reversed the head, add 1 to dh register. If the value of dh register after adding larger than or equal to 2, it's saying the original head is 1, one track of two sides read already. Otherwise the value of dh register smaller than 2, read this side indicating by dh register, jump to $readloop$ segmentation.

So the next step is moving a cylinder, add 1 to register ch. Otherwise the value of dh register smaller than 2, read this side indicating by dh register, jump to $readloop$ segmentation. After ch register add 1, if it's smaller than 10, jump to $readloop$, otherwise end loading floppy to memory process, for we only load ten cylinders of floppy.

3.1.4 Codes and Comments of Boot Loader

```
; read ten cylinders to memory begin with 0x8200.
; read order:
        ; C0-H0-S1 --- C0-H0-S18
        ; C0-H1-S1 --- C0-H0-S18
        ; C1-H0-S1 --- C1-H0-S18
        ; C1-H1-S1 --- C1-H1-S18
        ;          ...
        ; C9-H1-S1 --- C9-H1-S18
        ; C is cylinder, H is head, S is sector.
        ; total 10 * 2 * 18 * 512 = 184320Byte = 180KB.
        ; begin with 0x8200, end with 0x34fff in memory.

```

```
13          CYLS equ 10 ; read 10 cylinders,
14
15  org 0x7c00 ; load the program to address 0x7c00.
16          jmp entry
17
18          ; The next codes specify the format of standard FAT12 floppy disk.
19  db 0x90 ;db is the abbreation of "define byte", it literally places that byte
20          ; right there in the executable.
21  db "RONGBOOT" ;The name of boot sector, must be 8 byte.
22  dw 512 ; the size of every sector, must be 512 byte.
23  db 1 ; the size of cluster, must be 1.
24  dw 1 ; the start point of FAT, 1 general case.
25  db 2 ; the number of FAT, must be 2.
26  dw 224 ; the size of root directory, 224 in general.
27  dw 2880 ; the size of this floppy disk, must be 2880.
28  db 0xf0 ; the kind of disk.
29  dw 9 ; the length of FAT.
30  dw 18 ; how many sectors in one track, must be 18.
31  dw 2 ; the number of head, must be 2.
32  dd 0 ; no partion, must be 0.
33  dd 2880 ; the size if re-writer one time.
34  db 0,0,0x29 ; just fixed, no meaning.
35  dd 0xffffffff
36  db "RONGBOOTOS " ; the name of disk.
37  db "FAT12   " ; the name of disk formate.
38  resb 18 ; reserved 18 byte.
39  ; end FAT12 formate.
40
41
42  entry:
43          mov ax, 0 ; init the registers.
```

```
44          mov ss, ax ; can not directly write ss segment register.
45          mov sp, 0x7c00 ; the instructions of this program
46          ; loaded to 0x7c00 in memory, so sp=0x7c00, from here
47          ; to execute.
48
49          mov ds, ax
50
51          mov si, msg_init ; show some init message.
52          jmp init
53
54
55  init:
56          mov al, [si]
57          add si, 1 ; increment by 1.
58          cmp al, 0
59          je load ; if al == 0, jmp to load, the msg_init info displayed.
60  ; the lastest character is null character, coding in 0.
61
62          mov ah, 0x0e ; write a character in TTY mode.
63          mov bx, 15   ; specify the color of the character.
64          int 0x10 ; call BIOS function, video card is number 10.
65          jmp init
66  ;show some init messages.
67
68
69  msg_init:
70  db 0x0a ; new line
71  db 0x0d
72  db "Copyright: GPL"
73  db 0x0a
74  db 0x0d
```

```
75  db "Author: Qiyuan Pu"
76  db 0x0a
77  db 0x0d
78  db "https://github.com/Puqiyuan/RongOS"
79  db 0x0a
80  db 0x0d
81  db "IPL is loading, please waiting..."
82  db 0x0a
83  db 0x0d
84  db "......"
85
86
87  load:
88          mov ax, 0
89          mov ax, 0x0820 ; load C0-H0-S2 to memory begin with 0x0820.
90          mov es, ax
91          mov ch, 0 ; cylinder 0.
92          mov dh, 0 ; head 0.
93          mov cl, 2 ; sector 2.
94
95
96  readloop:
97          mov si, 0 ; si register is a counter, try read a sector
98  ; five times.
99
100
101 retry:
102         mov ah, 0x02 ; parameter 0x02 to ah, read disk.
103         mov al, 1 ; parameter 1 to al, read disk.
104         mov bx, 0
105         mov dl, 0x00 ; the number of driver number.
```

```
106         int 0x13 ; after prepared parameters, call 0x13 interrupted.
107
108         jnc next ; if no carry read next sector.
109         add si, 1 ; tring again read sector, counter add 1.
110         cmp si, 5 ; until five times
111         jae error ; if tring times large than five, failed.
112
113         ; reset the status of floppy and read again.
114         mov ah, 0x00
115         mov dl, 0x00
116         int 0x13
117         jmp retry
118
119
120 next:
121         mov ax, es
122         ; we can not directly add to es register.
123         add ax, 0x0020 ; add 0x0020 to ax
124         mov es, ax ; the memory increase 0x0020 * 16 = 512 byte.
125         ; size of a sector.
126         add cl, 1 ; sector number add 1.
127         cmp cl, 18 ; one track have 18 sector.
128         jbe readloop ; jump if below or equal 18, read the next sector.
129         mov cl, 1 ; cl number reset to 1, ready to read the other side.
130         add dh, 1 ; the other side of floppy.
131         cmp dh, 2 ; only two sides of floppy.
132         jb readloop ; if dh < 2, read 18 sectors of the other sides
133         ; of floppy.
134         mov dh, 0 ; after finished read the other side, reset head to 0.
135         add ch, 1 ; two sides of a cylinder readed, add 1 to ch.
136         cmp ch, CYLS ; read 10 cylinders.
```

```
137         jb readloop
138         jmp correct ; if 10 cylinders readed, show correct message.
139 fin:
140         hlt ; halt the cpu.
141         jmp fin
142
143
144 error:
145         mov si, msg
146
147
148 correct:
149         mov si, msg_corr
150
151
152 putloop:
153         mov al, [si]
154         add si, 1
155         cmp al, 0
156         mov [0x0ff0], ch
157         je 0xc200
158         mov ah, 0x0e
159         mov bx, 15
160         int 0x10
161         jmp putloop
162
163
164 msg_corr:
165 db 0x0a
166 db 0x0d
167 db 0x0a
```

```
168 db 0x0d
169 db "OK: IPL loaded"
170 db 0x0a
171 db 0x0d
172 db 0
173 msg:
174 db 0x0a
175 db "IPL load error"
176 db 0x0a
177 db 0
178 resb 0x7dfe-$
179 db 0x55, 0xaa ; the sector end with 0x55 0xaa, the sector is
180         ;boot sector.
```

3.1.5 Running Result

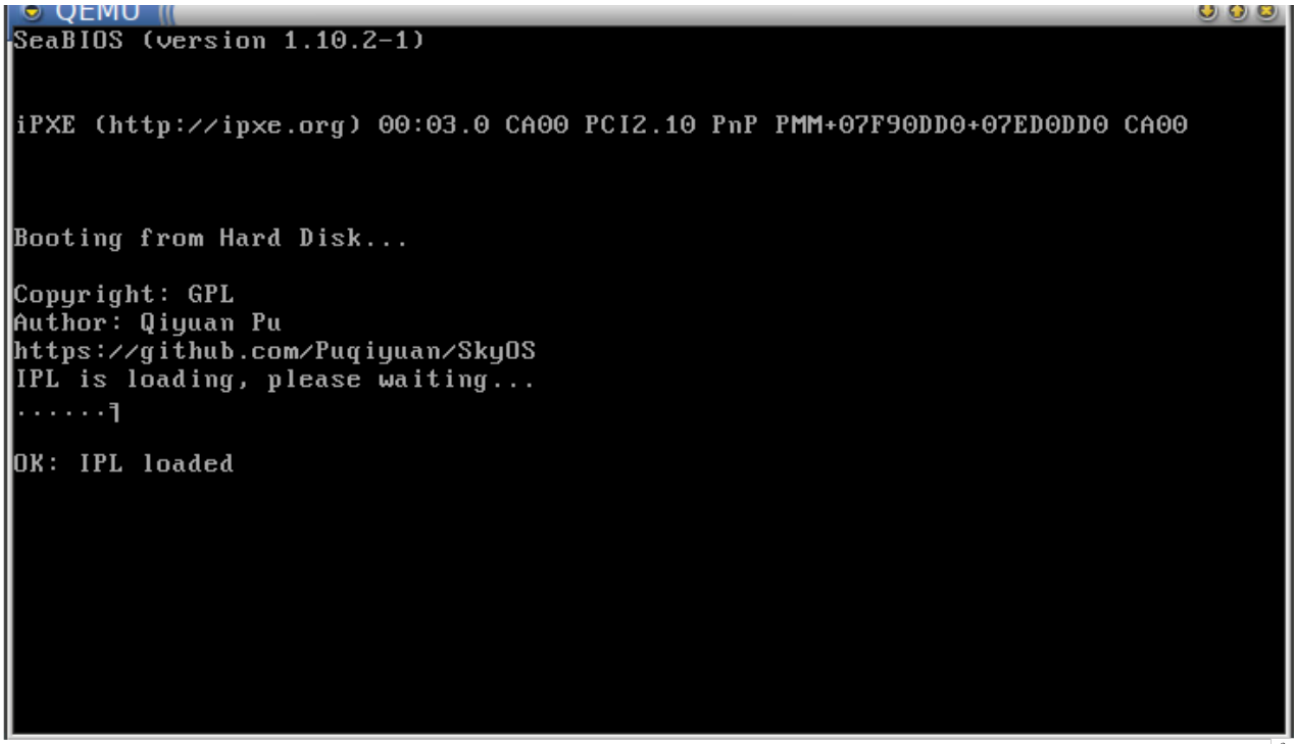

图 3-3 Running Result of Boot Loader

3.2 32-bit Mode and Import C Codes

3.3 Screen Display and Text

3.4 Control Mouse

3.5 Memory Management

3.6 Making Window

3.7 Timer

3.8 Multitasking

3.9 Command Line Window

3.10 API

3.11 OS Protection

3.12 Graphics Processing

3.13 Window Operation

3.14 Application Protection

3.15 File Operation

3.16 Some Applications

3.17 Prospects and Shortages

参考文献

[1] 国务院。*中国制造 2025*，2015-05。。

[2] WiKipedia. *Operating System*, 2017-08..

[3] 川合秀实. *30 天自制操作系统*. 人民邮电出版社, 2012-08.

指导教师简介

王晓林，男，49 岁，硕士，讲师，毕业于英国格林尼治大学，分布式系统专业，现任西南林业大学计信学院教师，执教 Linux、操作系统、网络技术等方面的课程，有丰富的 Linux 教学和系统管理经验。

致　谢

首先我想感谢我的老师，王晓林。大学期间，他给了我很多指导，包括专业方面和上大学的意义等。很多时候，他对学生的要求看起来都是不近情理的，但正是通过这个“痛苦”的过程，我锻炼了坚强的意志，和战胜困难的信心。谢谢你，王老师。我最想感谢的是我的女友，她容忍我在完成这个设计时的很多个夜晚不陪她，给我支持，鼓励我，不抱怨。所以我愿意把这个简单操作系统命名为 RongOS, 蓉便是她名字的最后一个字。谢谢你，我最亲爱的。