

书名、作者、ISBN

购书单 电子图书 豆瓣书店 2021年度榜单 2021书影音报告 购物车

x86汇编语言



作者: 李忠 / 王晓波 / 余洁

出版社: 电子工业出版社

副标题: 从实模式到保护模式

出版年: 2013-1

页数: 375

定价: 56.00元

装帧: 平装

ISBN: 9787121187995

豆瓣评分

9.2 256人评价

5星	72.7%
4星	23.8%
3星	2.7%
2星	0.4%
1星	0.4%

想读 在读 读过 评价: ☆☆☆☆☆

写笔记 写书评 加入购书单 分享到 推荐

内容简介 · · · · · ·

《x86汇编语言:从实模式到保护模式》采用开源的NASM汇编语言编译器和VirtualBox虚拟机软件,以个人计算机广泛采用的Intel处理器为基础,详细讲解了Intel处理器的指令系统和工作模式,以大量的代码演示了16 / 32 / 64位软件的开发方法,介绍了处理器的16位实模式和32位保护模式,以及基本的指令系统。

《x86汇编语言:从实模式到保护模式》是一本有趣的书,它没有把篇幅花在计算一些枯燥的数学题上。相反,它教你如何直接控制硬件,在不借助于BIOS、DOS、Windows、Linux或者任何其他软件支持的情况下来显示字符、读取硬盘数据、控制其他硬件等。《x86汇编语言:从实模式到保护模式》可作为大专院校相关专业学生和计算机编程爱好者的教程。

在线试读：

 得到

目录 · · · · · ·

目录

第1部分 预备知识

第1章 十六进制计数法 3

1.1 二进制计数法回顾 3

1.1.1 关于二进制计数法 3

1.1.2 二进制到十进制的转换 4

1.1.3 十进制到二进制的转换 4

1.2 十六进制计数法 5

1.2.1 十六进制计数法的原理 5

1.2.2 十六进制到十进制的转换 6

1.2.3 十进制到十六进制的转换 6

1.2.4 为什么需要十六进制 6

1.3 使用Windows计算器方便你的学习过程 8

本章习题 9

第2章 处理器、内存和指令 10

2.1 最早的处理器 10

2.2 寄存器和算术逻辑部件 10

2.3 内存存储器 12

2.4 指令和指令集 14

2.5 古老的Intel 8086处理器 16

2.5.1 8086的通用寄存器 16

2.5.2 程序的重定位难题 16

2.5.3 内存分段机制 19

2.5.4 8086的内存分段机制 21

本章习题 24

第3章 汇编语言和汇编软件 25

3.1 汇编语言简介 25

3.2 NASM编译器 27

- 3.2.1 NASM的下载和安装 27
- 3.2.2 代码的书写和编译过程 27
- 3.2.3 用HexView观察编译后的机器代码 30
- 本章习题 31
- 第4章 虚拟机的安装和使用 32
 - 4.1 计算机的启动过程 32
 - 4.1.1 如何将编译好的程序提交给处理器 32
 - 4.1.2 计算机的加电和复位 33
 - 4.1.3 基本输入输出系统 33
 - 4.1.4 硬盘及其工作原理 34
 - 4.1.5 一切从主引导扇区开始 36
 - 4.2 创建和使用虚拟机 37
 - 4.2.1 别害怕，虚拟机是软件 37
 - 4.2.2 下载和安装Oracle VM VirtualBox 37
 - 4.2.3 虚拟硬盘简介 39
 - 4.2.4 练习使用FixVhdWr工具向虚拟硬盘写数据 40
- 第2部分 实模式
- 第5章 编写主引导扇区代码 45
 - 5.1 本章代码清单 45
 - 5.2 欢迎来到主引导扇区 45
 - 5.3 注释 46
 - 5.4 在屏幕上显示文字 46
 - 5.4.1 显卡和显存 46
 - 5.4.2 初始化段寄存器 49
 - 5.4.3 显存的访问和ASCII代码 49
 - 5.4.4 显示字符 51
 - 5.4.5 MOV指令的格式 52
 - 5.5 显示标号的汇编地址 54
 - 5.5.1 标号 54
 - 5.5.2 如何显示十进制数字 58
 - 5.5.3 在程序中声明并初始化数据 58
 - 5.5.4 分解数的各个数位 59
 - 5.5.5 显示分解出来的各个数位 63
 - 5.6 使程序进入无限循环状态 64
 - 5.7 完成并编译主引导扇区代码 66
 - 5.7.1 主引导扇区有效标志 66
 - 5.7.2 代码的保存和编译 67
 - 5.8 加载和运行主引导扇区代码 67
 - 5.8.1 把编译后的指令写入主引导扇区 67
 - 5.8.2 启动虚拟机观察运行结果 68
 - 5.9 程序的调试技术 68
 - 5.9.1 开源的Bochs虚拟机软件 68
 - 5.9.2 Bochs下的程序调试入门 69
 - 本章习题 75
- 第6章 相同的功能，不同的代码 76
 - 6.1 代码清单6-1 76
 - 6.2 跳过非指令的数据区 76
 - 6.3 在数据声明中使用字面值 77
 - 6.4 段地址的初始化 77
 - 6.5 段之间的批量数据传送 78
 - 6.6 使用循环分解数位 80
 - 6.7 计算机中的负数 81
 - 6.7.1 无符号数和有符号数 81
 - 6.7.2 处理器视角中的数据类型 85
 - 6.8 数位的显示 87
 - 6.9 其他标志位和条件转移指令 88
 - 6.9.1 奇偶标志位PF 88
 - 6.9.2 进位标志CF 89
 - 6.9.3 溢出标志OF 89
 - 6.9.4 现有指令对标志位的影响 90
 - 6.9.5 条件转移指令 90
 - 6.10 NASM编译器的\$和\$\$标记 92
 - 6.11 观察运行结果 93
 - 6.12 本章程序的调试 93
 - 6.12.1 调试命令“n”的使用 93
 - 6.12.2 调试命令“u”的使用 94
 - 6.12.3 用调试命令“info”察看标志位 96
 - 本章习题 97
- 第7章 比高斯更快的计算 98
 - 7.1 从1加到100的故事 98

- 7.2 代码清单7-1 98
- 7.3 显示字符串 98
- 7.4 计算1到100的累加和 99
- 7.5 累加和各个数位的分解与显示 99
 - 7.5.1 栈和栈段的初始化 99
 - 7.5.2 分解各个数位并压栈 101
 - 7.5.3 出栈并显示各个数位 103
 - 7.5.4 进一步认识栈 104
- 7.6 程序的编译和运行 105
 - 7.6.1 观察程序的运行结果 105
 - 7.6.2 在调试过程中察看栈中内容 106
- 7.7 8086处理器的寻址方式 107
 - 7.7.1 寄存器寻址 107
 - 7.7.2 立即寻址 107
 - 7.7.3 内存寻址 108
- 本章习题 112
- 第8章 硬盘和显卡的访问与控制 113
 - 8.1 本章代码清单 114
 - 8.2 用户程序的结构 114
 - 8.2.1 分段、段的汇编地址和段内汇编地址 114
 - 8.2.2 用户程序头部 117
 - 8.3 加载程序（器）的工作流程 120
 - 8.3.1 初始化和决定加载位置 120
 - 8.3.2 准备加载用户程序 121
 - 8.3.3 外围设备及其接口 122
 - 8.3.4 I/O端口和端口访问 123
 - 8.3.5 通过硬盘控制器端口读扇区数据 125
 - 8.3.6 过程调用 127
 - 8.3.7 加载用户程序 133
 - 8.3.8 用户程序重定位 134
 - 8.3.9 将控制权交给用户程序 137
 - 8.3.10 8086处理器的无条件转移指令 138
 - 8.4 用户程序的工作流程 140
 - 8.4.1 初始化段寄存器和栈切换 140
 - 8.4.2 调用字符串显示例程 141
 - 8.4.3 过程的嵌套 142
 - 8.4.4 屏幕光标控制 142
 - 8.4.5 取当前光标位置 143
 - 8.4.6 处理回车和换行字符 144
 - 8.4.7 显示可打印字符 145
 - 8.4.8 滚动屏幕内容 145
 - 8.4.9 重置光标 146
 - 8.4.10 切换到另一个代码段中执行 146
 - 8.4.11 访问另一个数据段 147
 - 8.5 编译和运行程序并观察结果 147
 - 本章习题 148
- 第9章 中断和动态时钟显示 149
 - 9.1 外部硬件中断 149
 - 9.1.1 非屏蔽中断 150
 - 9.1.2 可屏蔽中断 150
 - 9.1.3 实模式下的中断向量表 152
 - 9.1.4 实时时钟、CMOS RAM和BCD编码 154
 - 9.1.5 代码清单9-1 157
 - 9.1.6 初始化8259、RTC和中断向量表 157
 - 9.1.7 使处理器进入低功耗状态 159
 - 9.1.8 实时时钟中断的处理过程 160
 - 9.1.9 代码清单9-1的编译和运行 162
 - 9.2 内部中断 163
 - 9.3 软中断 163
 - 9.3.1 BIOS中断 163
 - 9.3.2 代码清单9-2 165
 - 9.3.3 从键盘读字符并显示 165
 - 9.3.4 代码清单9-2的编译和运行 165
 - 本章习题 166
- 第3部分 32位保护模式
- 第10章 32位x86处理器编程架构 169
 - 10.1 IA-32架构的基本执行环境 169
 - 10.1.1 寄存器的扩展 169
 - 10.1.2 基本的工作模式 172
 - 10.1.3 线性地址 173

10.2 现代处理器的结构和特点	174
10.2.1 流水线	174
10.2.2 高速缓存	175
10.2.3 乱序执行	175
10.2.4 寄存器重命名	176
10.2.5 分支目标预测	177
10.3 32位模式的指令系统	178
10.3.1 32位处理器的寻址方式	178
10.3.2 操作数大小的指令前缀	179
10.3.3 一般指令的扩展	181
本章习题	184
第11章 进入保护模式	185
11.1 代码清单11-1	185
11.2 全局描述符表	186
11.3 存储器的段描述符	187
11.4 安装存储器的段描述符并加载GDTR	191
11.5 关于第21条地址线A20的问题	193
11.6 保护模式下的内存访问	195
11.7 清空流水线并串行化处理器	199
11.8 保护模式下的栈	200
11.8.1 关于栈段描述符中的界限值	200
11.8.2 检验32位下的栈操作	201
11.9 程序的运行和调试	202
11.9.1 运行程序并观察结果	202
11.9.2 处理器刚加电时的段寄存器状态	203
11.9.3 设置PE位后的段寄存器状态	205
11.9.4 JMP指令执行后的段寄存器状态	205
11.9.5 察看全局描述符表GDT	206
11.9.6 察看控制寄存器的内容	207
本章习题	207
第12章 存储器的保护	208
12.1 代码清单12-1	208
12.2 进入32位保护模式	208
12.2.1 话说mov ds,ax和mov ds,edx	208
12.2.2 创建GDT并安装段描述符	209
12.3 修改段寄存器时的保护	211
12.4 地址变换时的保护	213
12.4.1 代码段执行时的保护	213
12.4.2 栈操作时的保护	214
12.4.3 数据访问时的保护	216
12.5 使用别名访问代码段对字符排序	217
12.6 程序的编译和运行	219
本章习题	220
第13章 程序的动态加载和执行	221
13.1 本章代码清单	222
13.2 内核的结构、功能和加载	222
13.2.1 内核的结构	222
13.2.2 内核的加载	223
13.2.3 安装内核的段描述符	225
13.3 在内核中执行	229
13.4 用户程序的加载和重定位	230
13.4.1 用户程序的结构	230
13.4.2 计算用户程序占用的扇区数	232
13.4.3 简单的动态内存分配	233
13.4.4 段的重定位和描述符的创建	234
13.4.5 重定位用户程序内的符号地址	238
13.5 执行用户程序	242
13.6 代码的编译、运行和调试	243
本章习题	244
第14章 任务和特权级保护	245
14.1 任务的隔离和特权级保护	246
14.1.1 任务、任务的LDT和TSS	246
14.1.2 全局空间和局部空间	248
14.1.3 特权级保护概述	250
14.2 代码清单14-1	257
14.3 内核程序的初始化	257
14.3.1 调用门	258
14.3.2 调用门的安装和测试	261
14.4 加载用户程序并创建任务	264
14.4.1 任务控制块和TCB链	264

- 14.4.2 使用栈传递过程参数 266
- 14.4.3 加载用户程序 268
- 14.4.4 创建局部描述符表 269
- 14.4.5 重定位U-SALT表 270
- 14.4.6 创建0、1和2特权级的栈 271
- 14.4.7 安装LDT描述符到GDT中 271
- 14.4.8 任务状态段TSS的格式 272
- 14.4.9 创建任务状态段TSS 276
- 14.4.10 安装TSS描述符到GDT中 276
- 14.4.11 带参数的过程返回指令 277
- 14.5 用户程序的执行 278
- 14.5.1 通过调用门转移控制的完整过程 278
- 14.5.2 进入3特权级的用户程序的执行 281
- 14.5.3 检查调用者的请求特权级RPL 284
- 14.5.4 在Bochs中调试程序的新方法 286
- 本章习题 286
- 第15章 任务切换 287
- 15.1 本章代码清单 287
- 15.2 任务切换前的设置 287
- 15.3 任务切换的方法 289
- 15.4 用call/jmp/iret指令发起任务切换的实例 292
- 15.5 处理器在实施任务切换时的操作 296
- 15.6 程序的编译和运行 298
- 本章习题 299
- 第16章 分页机制和动态页面分配 300
- 16.1 分页机制概述 301
- 16.1.1 简单的分页模型 301
- 16.1.2 页目录、页表和页 305
- 16.1.3 地址变换的具体过程 307
- 16.2 本章代码清单 308
- 16.3 使内核在分页机制下工作 309
- 16.3.1 创建内核的页目录表和页表 309
- 16.3.2 任务全局空间和局部空间的页面映射 314
- 16.4 创建内核任务 319
- 16.4.1 内核的虚拟内存分配 319
- 16.4.2 页面位映射串和空闲页的查找 320
- 16.4.3 创建页表并登记分配的页 323
- 16.4.4 创建内核任务的TSS 324
- 16.5 用户任务的创建和切换 325
- 16.5.1 多段模型和段页式内存管理 325
- 16.5.2 平坦模型和用户程序的结构 327
- 16.5.3 用户任务的虚拟地址空间分配 328
- 16.5.4 用户程序的加载 329
- 16.5.5 段描述符的创建（平坦模型） 332
- 16.5.6 重定位U-SALT并复制页目录表 333
- 16.5.7 切换到用户任务执行 334
- 16.6 程序的编译、执行和调试 336
- 16.6.1 本章程序的编译和运行方法 336
- 16.6.2 察看CR3寄存器的内容 337
- 16.6.3 察看线性地址对应的物理页信息 337
- 16.6.4 察看当前任务的页表信息 338
- 16.6.5 使用线性（虚拟）地址调试程序 339
- 本章习题 339
- 第17章 中断和异常的处理与抢占式多任务 340
- 17.1 中断和异常 340
- 17.1.1 中断和异常概述 340
- 17.1.2 中断描述符表、中断门和陷阱门 343
- 17.1.3 中断和异常处理程序的保护 345
- 17.1.4 中断任务 347
- 17.1.5 错误代码 348
- 17.2 本章代码清单 349
- 17.3 内核的加载和初始化 349
- 17.3.1 彻底终结多段模型 349
- 17.3.2 创建中断描述符表 352
- 17.3.3 用定时中断实施任务切换 354
- 17.3.4 8259A芯片的初始化 359
- 17.3.5 平坦模型下的字符串显示例程 362
- 17.4 内核任务的创建 362
- 17.4.1 创建内核任务的TCB 362
- 17.4.2 宏汇编技术 364

17.5 用户任务的创建 366

17.5.1 准备加载用户程序 366

17.5.2 转换后援缓冲器的刷新 367

17.5.3 用户任务的创建和初始化 368

17.6 程序的编译和执行 370

本章习题 371

附录 I 本书用到的x86指令及其页码 372

附录II 本书用到的重要图表及其页码 374

..... (收起)

喜欢读"x86汇编语言"的人也喜欢的电子书

支持 Web、iPhone、iPad、Android 阅读器



Python源码剖析

17.99元



编程之美

19.28元

喜欢读"x86汇编语言"的人也喜欢



计算机系统要素



自制编译器



汇编语言 (第3版)



Linux二进制分析



编译器设计 (第2版)



操作系统导论



编程语言实现模式



Orange'S:一个操作系统的实现



Unix/Linux编程实践教程



Manchus and Han

短评 (全部 88 条)

热门 / 最新 / 好友

- 阅微草堂

2022-04-18 15:19:05

0 有用
- 冯业浩

2014-11-18 12:10:06

1 有用
- 鲜鱼巷口

2019-01-28 18:32:56

9 有用
- 深海有大鱼

2020-07-29 16:53:34

0 有用
- 开头几章的视频地址：<https://www.bilibili.com/video/BV1xE411N74T?p=17> nasm c11_mbr.asm -f bin -o c11_mbr.bin
中间使用一个硬盘写入的命令即可 qemu-system-i386 -hda c11_mbr.bin 入门操作系统的一些常见问题：BIOS作用，引导扇区，内存的物理组成，硬盘的操作和原理，显卡和显示器的操作... (展开)
- 本书→intel微处理器(书名)→intel开发人员帮助手册
- 很难评价，从里面补充了不少x86汇编的知识，但是没有真正的运行过书上的代码，尤其后半部分的代码，

千山落叶飞2018-10-13 15:01:525 有用


比王爽老师那本讲的更好！最喜欢讲负数的那段，简单的-1=0-1=11111111b,-128=127+1=10000000b溢出成了最小\值。不像课本上照本宣科地解释各种原码，反码，补码。中华文化里的物极必反，否极泰来这么简单的思想都被编课本的人吃了？

> 更多短评 88 条

x86汇编语言的书评 ······ (全部 4 条)

我要写书评

热门 / 最新 / 好友


 郑梓男2020-04-28 12:00:07

其实是本写操作系统的书

没想到写长评的人如此之少。我是买的二手,很便宜,现在书可是越来越贵了,也只能买买二手。书里后半部分基本没有笔记,可能原主看一半就弃了吧,正好我把后半部分给读完,完美。我是读完王爽老师的《汇编语言》直接读这本书的,于是此书前半部分,我基本是直接略过了,从第10章... (展开)

△ 14

▽ 2 回应


 tome2013-01-13 11:44:52

x86汇编语言

恳请创建者更改为《x86汇编语言：从实模式到保护模式》.不然就违背了作者本身意图。大家可以加我的QQ：1658843124 进行讨论，我们一起互相学习，互相交流，也会有作者的亲自指点。谢谢大家 评论字数至于这么多吗？ (展开)

△ 7

▽ 1 回应


 房随成2019-09-18 17:50:04

汇编书评

国内有关保护模式的书看过几本。李忠的这本是最好的：层层递进，丝丝入扣。遵循王爽提过的知识屏蔽原则，用到什么讲什么，不需要提前“储备”一堆知识才开始写代码。理论知识与代码解释穿插进行，代码没有大段大段的印在书上，我是打印出来两相对应着看，不用翻来翻去的找，还... (展开)

△ 2

▽ 1 回应

 钝风2021-01-31 22:22:18

最佳汇编语言入门书籍

相比于其他将汇编语言的书，这本书的优势在于两点：一、理论与实践的结合，实际动手编写汇编语言程序并在Bochs虚拟机上面运行观察程序的输出/效果；二、突出强调了汇编语言是底层硬件和操作系统的结合点，并介绍了中断、页表、进程切换等核心操作系统概念，为读者进一步学习并... (展开)

△

▽ 0 回应

> 更多书评 4篇

读书笔记 ······ (共9篇)

按有用程度按页码先后最新笔记

我来写笔记

- 

第197页 保护模式下的内存访问

龙三 (的日常)



段选择子

2019-06-09 12:37:091 人喜欢
- 


第188页 存储器的段描述符格式

龙三 (的日常)



存储器的段描述符格式：

2019-06-02 22:18:321 人喜欢




第277页 安装 TSS 描述符到 GDT

龙三 (的日常)

TSS 描述符:

2019-06-13 11:52:11



第272页 安装 LDT 描述符到 GDT

龙三 (的日常)

LDT 描述符:

2019-06-13 11:32:12

> 更多读书笔记 (共9篇)

论坛 ·····

在这本书的论坛里发言