程序设计基础(C语言)与安全

任课老师：赵奎 赵辉 方智阳

网络空间安全学院

2022级

课程项目

之

安全项目

进度安排

校历周/时间	标题	内容
3/2022-09-12	作业 3：by Word Demo CPU 剖析	来自于 OS 教材的一个例子
4/2022-09-21	作业 3 的评讲	对作业 3 的部分同学答案、 以及相关重点，进行了评讲
7/2022-10-12	安全项目启动	讲解了实验总览/实验来源等
8/2022-10-19	安全项目 -基础知识 1	Intel CPU 基础(寄存器和指令) 数据类型及其 VS 观察
10/2022-10-26	安全项目 -基础知识 2	Intel CPU 基础(寄存器和指令) 控制流/函数及其 VS 观察
11/2022-11-2	安全任务的说明	对前两个安全任务的说明提示

温故 0. 作业3-”Demo CPU的指令周期”的回顾与总结

1. Intel CPU的内部结构
2. Intel CPU的指令系统
3. Intel CPU的寻址方式
4. 实例演示
5.小结
6.课后作业

课程项目 之 安全项目 相关基础知识（上）

0.作业3-"Demo CPU的指令周期"的回顾与总结

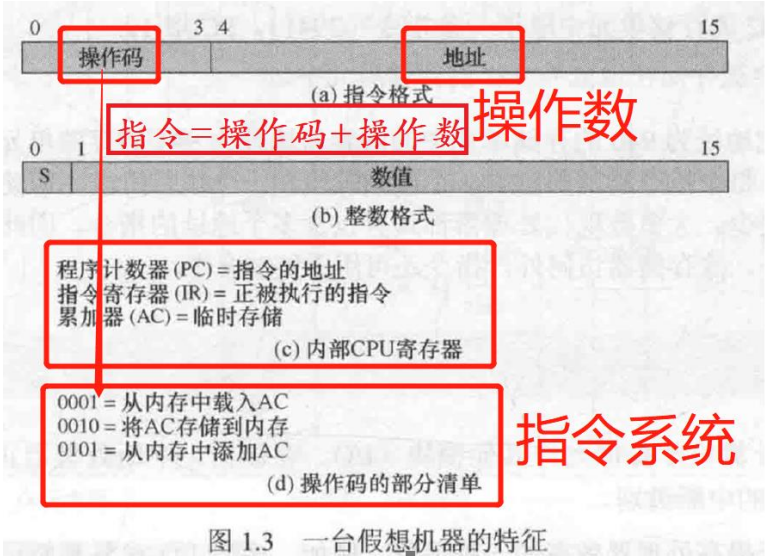


图 1.3 一台假想机器的特征

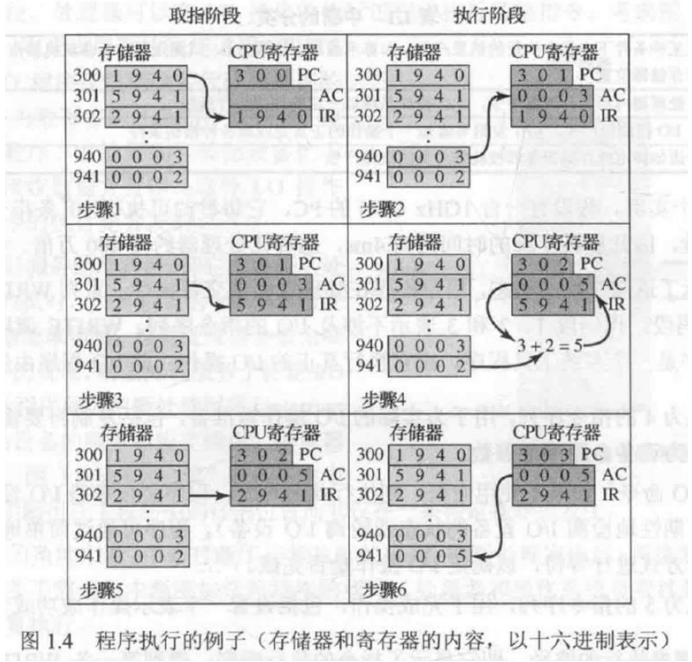
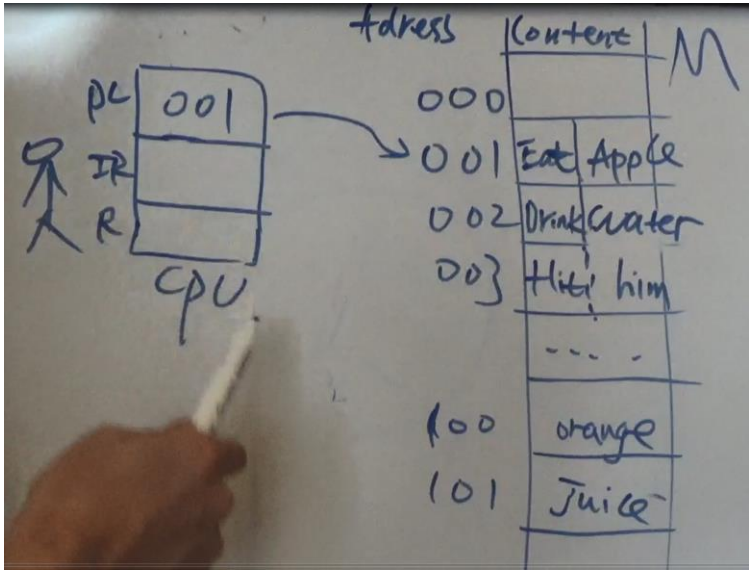


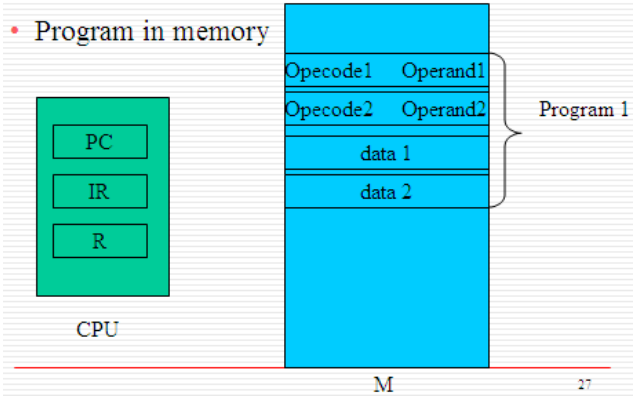
图 1.4 程序执行的例子（存储器和寄存器的内容，以十六进制表示）

备注： 本作业的关键点

- ✓ 指令的构成：指令 = 操作码/Opecode + 操作数/Operand
- ✓ 指令的执行：指令周期：取指 + 解析/运行

0.作业3-"Demo CPU的指令周期"的回顾与总结





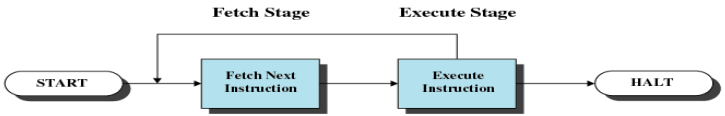


Figure 1.2 Basic Instruction Cycle

补充：本作业的生活化讲解

- ✓ 指令的构成：指令 = 动词+ 名词
- ✓ 指令的执行：指令周期：取指/从M到CPU + 解析/运行by CPU的运算器

课程项目 之 安全项目 相关基础知识（上）

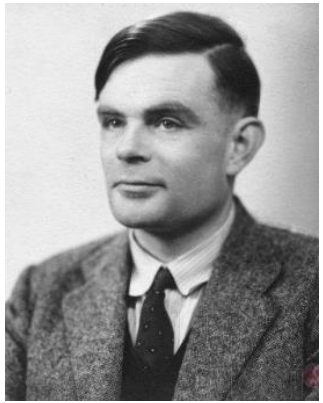
0.作业3-"Demo CPU的指令周期"的回顾与总结

进一步总结

- CPU＋M的框架：
  - ✓ CPU的内部结构：如寄存器等
  - ✓ M的区域划分：如Code/Data等
- CPU ←→ M的指令周期：
  - ✓ 取指：在PC寄存器的指引下
  - ✓ 解析/执行指令：依据：操作码/Opecode
  - ✓ 解析/执行指令：对象：操作数/Operand

备注： 对比：不同CPU

- ✓ 同，如左的标题所示
- ✓ 异：？



0.作业3-"Demo CPU的指令周期"的回顾与总结

进一步总结

- CPU＋M的框架：
  - ✓ **CPU的内部结构：如寄存器等**
  - ✓ M的区域划分：如Code/Data等
- CPU ←→ M的指令周期：
  - ✓ 取指：在PC寄存器的指引下
  - ✓ **解析/执行指令：依据：操作码/Opecode**
  - ✓ **解析/执行指令：对象：操作数/Operand**

备注： 对比：不同CPU
✓ 同，如左的标题所示
✓ 异：**如左所示**

知新

0. 作业3-"Demo CPU的指令周期"的回顾与总结

1. Intel CPU的内部结构

2. Intel CPU的指令系统

3. Intel CPU的寻址方式

4. 实例演示

5.小结

6.课后作业

进一步总结

- CPU + M的框架：
  - ✓ 1 CPU的内部结构：如寄存器等
  - ✓ M的区域划分：如Code/Data等
- CPU ←→ M的指令周期：
  - ✓ 取指：在PC寄存器的指引下
  - ✓ 2 解析/执行指令：依据：操作码/Opecode
  - ✓ 3 解析/执行指令：对象：操作数/Operand

备注：对比：不同CPU
- ✓ 同，如左的标题所示
- ✓ 异：如左所示

课程项目

之

安全项目

相关基础知识（上）

目录

0. 作业3-”Demo CPU的指令周期”的回顾与总结

知新 1. Intel CPU的内部结构

2. Intel CPU的指令系统

3. Intel CPU的寻址方式

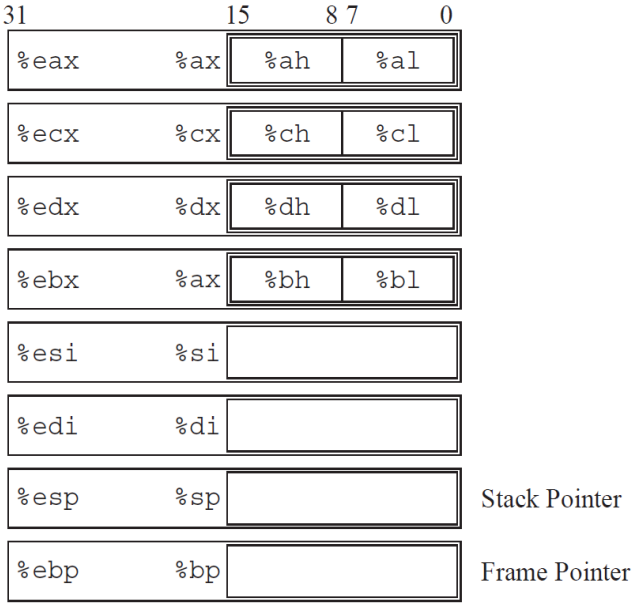
4. 实例演示

5.小结

6.课后作业

1.Intel CPU的内部结构

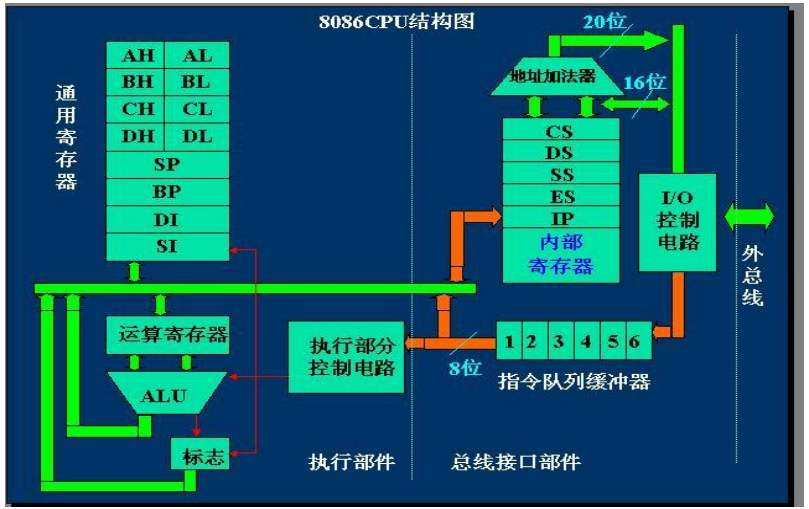
- 整数寄存器：8个
- 名字/size：(其中?可以是ABCD) [大小写均可]
  - ✓ 8位：?H/?L
  - ✓ 16位：?X
  - ✓ 32位：E?X



备注： 参见CSAPP 中文版 2nd的p112的图3-2

1.Intel CPU的内部结构

- PC寄存器：CS/IP
- ALU：算术逻辑单元/运算器
- 标志寄存器：某些bit有特殊的含义
  - ✓ CF位：
  - ✓ ZF位：
  - ✓ OF位：
  - ✓ ..



备注： 图片：来自于网络

关于标志寄存器：https://blog.csdn.net/abc123lzf/article/details/109258188

课程项目 之 安全项目

相关基础知识（上）

目录

0. 作业3-”Demo CPU的指令周期”的回顾与总结

1. Intel CPU的内部结构

知新 2. Intel CPU的指令系统

3. Intel CPU的寻址方式

4. 实例演示

5.小结

6.课后作业

2.Intel CPU的指令系统

本课程采用了微软/VS风格

- 数据移动指令：**MOV**
  - ✓ 操作数两个：源，目的
  - ✓ 兼有：从 CPU -> M、 M-> CPU，以及CPU的寄存器之间
  - ✓ 一致性：源和目的size一样
- 算术运算指令：
  - ✓ **ADD**：加法
  - ✓ **SUB**：减法
  - ✓ …

备注：本次课，暂时就了解这三个指令

CSAPP章节：3.4.2/3.5.2节

参考资料：https://max.book118.com/html/2017/0605/111843200.shtm

3.Intel CPU的寻址方式

本课程采用了微软/VS风格

- 寄存器寻址：
  - ✓ 如：MOV EAX, EBX
  - ✓ 如：ADD EAX, EBX
- 立即数寻址：
  - ✓ 如：MOV EAX, 10
  - ✓ 如：ADD EAX, 10
- 直接寻址：
  - ✓ 如：MOV EAX, [10]
  - ✓ 如：ADD EAX, [10]

备注：本次课，暂时就了解这三种

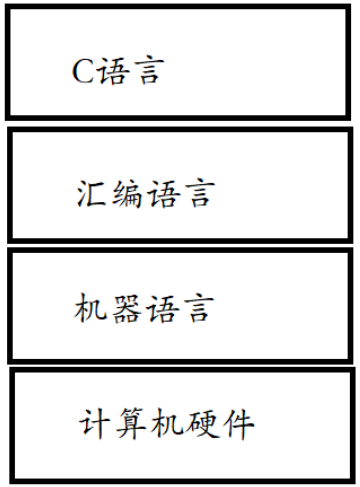
CSAPP章节：3.4.1节

参考资料：https://max.book118.com/html/2017/0605/111843200.shtm

课程项目 之 安全项目 相关基础知识（上）

4.实例演示

- 新建项目：Visual C++/空项目
- 添加文件：.c文件
- 编译：生成解决方案
- 运行：执行
- 调试：常用的窗口
  - ✓ CPU的寄存器
  - ✓ 常见变量
  - ✓ 内存
  - ✓ 反汇编



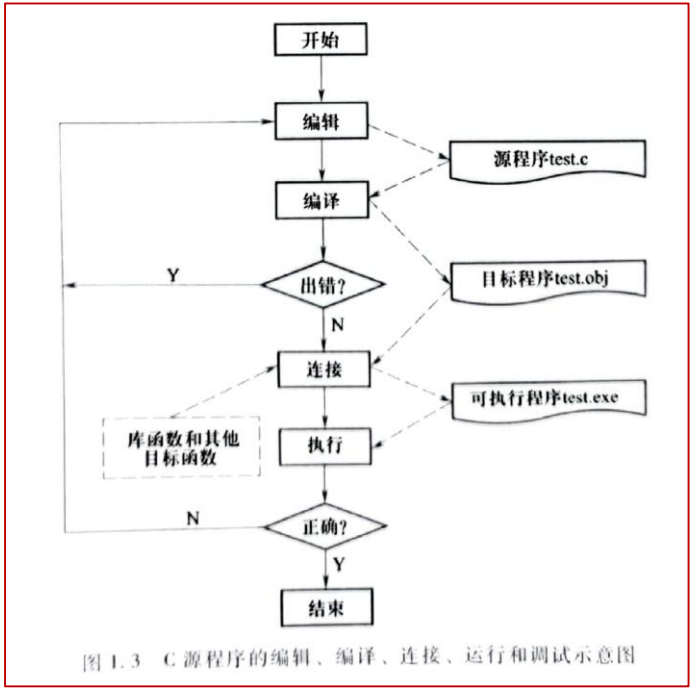


图 1.3 C 源程序的编辑、编译、连接、运行和调试示意图

CSAPP章节：2.1.6/3.2.2/3.2.3节 [备注：后面两个偏难]

备注：采用了VS2017版本，其他版本的操作大同小异

5.小结

无需记忆，通过实践理解

- Intel CPU：
  - ✓ 内部结构：如常用寄存器
  - ✓ 指令系统：三个
  - ✓ 寻址方式：三种
- Memory：
  - ✓ 地址和内容：以字节为单位编址；包括了Code区域和Data区域
  - ✓ 简单数据类型：如char/int的存储 CSAPP章节：2.1.3
  - ✓ 相关规则：如字的地址、小端等 CSAPP章节：2.1.4

备注：CSAPP 2nd 的相关章节
- ✓ Chap2: 第2.0到2.1节(到2.1.4)
- ✓ Chap3: 第3.0-3.4节

课程项目之安全项目相关基础知识（上）

6.课后作业 [自行完成，无需提交]

- 实践：通过VS+实例，熟悉掌握其调试功能（常用窗口）
- 更多：Intel CPU的相关知识
  - ✓ 1）其他常用的寄存器：如FLAG、如**ESP/EBP**等
  - ✓ 2）其他常用的指令：如算术/逻辑/位运算、跳转、循环和**函数**等
  - ✓ 3）其他常用的寻找方式：如基址/变址、如**堆栈**等

备注： 分以上是为了下周的（下）提前预习

备注： CSAPP 2nd 的相关章节
- ✓ Chap2: 2.1节(2.1.4后)
- ✓ Chap3: 第3.5-3.10/12节

更多资料：
网址1：
https://juejin.cn/post/6844903554206056455?share_token=db7ad134-001e-43cf-a792-cb05ff5397dc
网址2：
https://www.cs.virginia.edu/~evans/cs216/guides/x86.html?share_token=b9657a51-5f2e-4c3d-8f9f-3d94735c7337

感谢各位同学

Question?