《汇编语言与接口》考试复习

张华平 副教授 博士
Email: kevinzhang@bit.edu.cn
Website: http://www.nlpir.org/
@ICTCLAS张华平博士
大数据搜索与挖掘实验室（wSMS@BIT）
2019-6

北京理工大學 BEIJING INSTITUTE OF TECHNOLOGY

基本信息

期末考试：

6-25日 9:30-11:30 地点： 信3004，3006

复习范围：

课件及教材相关内容，尤其是重点范围

答疑：

在微信群问，我会尽快答，方便更多同学看到

实验报告：

各班学习委员收齐，7.2日前，Email给kevinzhang@bit.edu.cn。

复习重点：

- 1.3 内存及存储器访问
  - 逆袭存储；存储器基本概念：字节、字、双字、存储顺序（逆序存放）；LSB=0等
  - **数据表示：01　FDH(错误)→0FDH**

了解掌握：

- 1.1 微处理器及其性能指标、芯片组、接口等
  - 主频=外频×倍频
  - 2条DDR 400内存条，工作在200MHz频率下，每个时钟可以传送2次64位数据，求单/双通道带宽

200M×2×64÷8 = 3200MB/s = 3.2 GB/s。

习题：　1. 7-10

复习重点：

2.2 CPU工作模式

- 实模式；保护模式（支持多任务和特权级；页式存储；段式存储）；虚拟8086模式；特权0（最高，OS）,1,2,3

2.3 寄存器

- 寄存器名称、结构及用途，标志寄存器中CF、ZF、SF、OF、IF、DF的含义及用途。
- 保护模式：全局描述符表寄存器GDTR（高32位：基址+16位限长;最多2^13个描述符）；中断IDTR；局部LDTR(16位选择符)；任务TR；任务状态寄存器TSS；段选择符（16位；TI+RPL）

复习重点：

2.4 内存管理

- **实模式：分段管理，存储器寻址，20位物理地址的计算，段地址*10+offset。**
- 保护模式：段描述符（段地址32；限长20；DPL:描述符特权级；页式存储；每页4K）
- 虚拟地址到物理地址转换，16bit段选择符+32位offset；页式转换；
- PDBR:页目录基址寄存器；分页机制(10bit页目录索引+10位页表索引+12bit页面索引)

了解掌握：

- 2.5 任务
  - 任务状态段TSS；门（系统描述符；调用门；任务门）
- 2.6 保护
  - 数据访问的保护；对程序的保护；对输入输出的保护
  - 数据访问：DPL ≥ MAX(CPL, RPL)； CPL是当前正在运行的程序的特权级（CS）；DPL是描述符特权级；RPL是请求特权级。
  - 段间调用或跳转，需要检查限长，特权级CPL和DPL
    - CPL=DPL，允许跳转和调用。CPL<DPL，禁止。CPL>DPL，此时要检查段描述符的C位。如果C位为1，表示这是一致代码段,允许跳转和调用。

习题： 2.5;2.9;2.15;2.24;图2-40, 41, 42

重点复习：

- 3.1数据寻址方式；
- 3.2数据运算指令
- 3.3程序控制指令

了解掌握：

- 3.4 处理机控制指令
- 3.5 块操作指令

习题： 3. 3, 3. 4, 3. 6, 3. 9, 3. 24

需要掌握的指令

熟练掌握MOV指令的操作数限定（适用于大多数双操作数指令），注意部分指令对操作数或结果的特殊要求（以下用红色标注）。

熟练掌握以下常用指令：

1. 数据传送指令：MOV、PUSH、POP、XCHG、 IN、OUT、LEA、PUSHF、POPF

2. 二进制运算指令：ADD（什么时候计算无效？）、ADC、INC、SUB、SBB、DEC、CMP、MUL、 IMUL SRC、DIV、IDIV

3. 逻辑运算指令：AND、OR、NOT、XOR、TEST

需要掌握的指令（续）

5. 移位指令

SHL、SAL、SHR、SAR、ROL、ROR、RCL、RCR

6. 程序控制指令

转移指令（JMP及条件转移指令，条件？）、循环指令(LOOP：跳转；CX)、子程序指令：CALL、RET、RET n、中断指令：INT n、IRET

7. 处理机控制指令：

标志操作指令（对IF、DF、CF）及其应用场合、NOP指令

8. 串操作指令及其执行前的准备工作（结合程序片段）

重复前缀、DF、指针、MOVSB/W/D、STOSB/W/D、LODSB/W/D、CMPSB/W/D、SCASB/W/D

了解：3.4.2

第4章 汇编语言程序开发

重点复习：

- 4.1汇编语言编程基本知识
- 4.3.3 Windows汇编语言程序设计
- 4.4 分支与循环程序设计
- 4.5 浮点运算

了解掌握：

- 4.6 程序优化

习题： 4. 3, 4. 4, 4. 8

复习重点：

通过上机掌握
Debug的反汇编输出
Windbg的反汇编输出(PROG0412)
实模式，虚拟模式的程序框架

掌握：

① 熟练掌握数据定义、符号定义伪指令及部分汇编语言操作符

② 熟练编写简单的、完整的汇编语言源程序（注意DOS16、Windows32（控制台及窗口界面）的典型程序框架及其中的伪指令格式、功能、位置）

③ 实现数据的输入输出（printf、scanf、MessageBoxA）

④ 掌握上机操作（DOS16、Windows32常用汇编、连接命令）

⑤熟悉.EXE和.COM文件结构以及主要区别，熟练掌握.EXE结构程序框架。

SEGMENT/ENDS、ASSUME、PROC/ENDP、END、定义数据（DB、DW、DD）、ORG、EQU、＝、结构定义预置存取、.386、.model flat stdcall、invoke、include、includelib等。

算术操作符、返回值操作符(SEG、OFFSET、$)、属性操作符PTR

浮点寄存器FPU;finit;fld;fmul;fst;fcmp;

复习重点：

通过复习本章程序，掌握分支、循环程序设计

具体要求：

1. 掌握IF_THEN_ELSE程序设计
2. 掌握CASE结构程序设计
3. 掌握循环程序基本结构及其程序设计方法
4. 掌握统计、查找、插入、删除、排序等程序设计。

第5章 子程序设计

重点复习：

- 5.1子程序基本知识
- 5.2 参数传递
- 5.5 C语言程序的反汇编

了解掌握：

- 5.3子程序特殊应用
- 5.4模块化程序设计
- 5.6混合编程

习题： 5.1 5.7

第5章　子程序设计

重点：

1. 熟悉子程序设计方法，综合利用本章及前几章所学知识，进行子程序设计。
2. 掌握以下参数传递方法的子程序设计：寄存器、子程序直接访问同模块中的内存变量、[BP+N]方式从堆栈传递参数或参数地址
3. 掌握ASCII码←→十进制数、十进制数←→二进制数之间的代码转换程序
4. 掌握模块化程序的主、子模块程序结构
5. 掌握EXTRN、PUBLIC伪指令的格式、功能及应用场合。
6. 掌握多模块程序设计的上机步骤，注意LINK时与单模块的区别。
7. C语言反汇编：全局变量、局部变量、函数、指针

了解：缓冲区溢出攻击原理

第6章 存储系统与技术

重点复习：

- 6.1.1 Cache工作原理：
  - 局部性原理；贯通查找式；旁路读出式；Cache映射；替换
- 6.2 DDR读写时序
  - 图6-12；图6-13

了解掌握：

- 6.3.4 辅助存储器/扇区编址：<C，H，S>，0≤C≤nC−1，0≤H≤nH−1，1≤S≤nS，则L=[(C×nH + H)×nS]+S–1
- 6.3.7 SATA：SATA接口差分方式传输；NCQ技术: Native Command Queuing全速命令排队
- 不要求：固态硬盘

习题：6.1 6.3 6.4 6.8 6.9

第7章 总线技术

重点复习：

- 无

了解掌握：

- 7.2 PCI：图7-5
- 7.3 PCI-E总线
- 7.4 USB总线：图7-15线缆定义；
- 7.5 I^2C总线

习题： 7.6

第8章 接口技术

- 8.1.2 可编程串行通信
  - 波特率；数据传输效率；线路状态寄存器LSR,线路控制寄存器LCR（格式表不需要背）；例8.5，8.6
  - $f_{工作时钟} = f_{基准时钟} \div$ 除数锁存器 = 波特率 × 16 ； 例8.7
- 8.2 定时和计数及其应用
  - 图8-26 8254控制字格式（不需要背）；例8.12；8.13；图8-36；图8-37对应的程序

了解掌握：

- 8.1 概述: RS-232C与TTL
- 8.3 红外 8.4 Wi-Fi

习题： 8.9；8.12；8.14

重点复习：

- 9.4 可编程控制器8259
  - 初始化命令字ICW1-4；中断屏蔽操作命令字OCW1-3; 9.3 保护模式中断和异常的处理过程

了解掌握：

- 9.1 中断概述
  - 中断、异常（故障、 陷阱、中止）
- 9.2 实模式的处理过程
  - 中断向量表；
- 9.5【简单了解，不作要求】高级可编程中断控制器

  例题9.6~9.13

考试题型范围

1、选择 15*1
2、填空 20*1
3、简答 4*5
4、综合：10*3
5、编写：15*1

单项选择题（每道题1分，共10分）

- 3. 8086 CPU中断号为8的中断矢量存放在(　　)。
- A. 0FFFFH:0008H　　B. 0000H:0008H
- C. 0000H:0020H　　D. 0020H:0000H
- 4. 主程序从堆栈传递3个dword型参数给子程序，则子程序的返回指令应该是(　　)。
- A．RET 12　　B．RET 6
- C．IRET　　D．RET 3
- 3、计算机采用的是标准TTL（Transistor-Transistor Logic）。（）为低电平，表示逻辑0。
- A. 0V～0.4V　　B. -5V～-15V
- C. +5V～+15V　　D. ＋2.4V～＋5V

填空题（每空1分，共20分）

- 1. 若EBX寄存器的值为1A0FC50EH，则BX寄存器值为_____H，BL寄存器值为_____H。
- 2. 地址总线宽度决定了CPU的寻址能力，如果地址总线宽度为8位，则CPU的寻址能力为_____Byte；如果地址总线为34位，则CPU的寻址能力为_____Byte。
- 3. 段间调用或跳转，需要检查限长，特权级CPL和DPL；段描述符C位为0，表示这是不一致代码段,允许跳转和调用的条件是：_____

简答题（共25分）

- 1. 请写出至少4种对EDX寄存器清零的指令。
- 2. 汇编语言中根据两个无符号数比较结果实现转移的条件转移指令中，有这样一条指令JA/JNBE LABEL(高于/不低于等于转移 cf=0and zf=0) ,JL(SF!=OF)/JG(ZF=0 and SF=OF)，其对标志位的测试条件是什么？解释该测试条件和功能的对应关系。
- 3. 如何优化EBX=EAX-30
  - MOV EBX,EAX; SUB EBX 30==LEA EBX,[EAX-30]
- 4.不允许实现乘法指令，实现Y=X*20
- 5.保护模式下，假定运行分页，运行在LDT上，如何实现DS:[EBX]虚拟地址如何生成物理地址

综合题（每道题10分*3）

1. 补全下面空格处的语句，使得程序实现统计F000:0000处的32个字节中，大小在[32,128]（注：该区间为闭区间）范围内数据的个数。

```
        MOV AX，0F000H
        MOV DS，AX
        MOV BX，0
        MOV DX，0
        MOV CX，32
S1:     MOV AL，[BX]
        CMP AL，32
        _____________
        CMP AL，128
        _____________
        INC DX
S2:     INC BX
        LOOP S1
```

综合题（10分*3）

- PROG0605!subproc:
- 00401020 55 push ebp
- 00401021 8bec mov ebp,esp
- 00401038 8b4508 mov eax,dword ptr [ebp+8]
- 0040103b 0faf450c imul eax,dword ptr [ebp+0Ch]
- 00401044 5d pop ebp
- 00401045 c20800 ret 8

问题1：子程序subproc的参数调用规则为_____。(2分)
A. cdecl B. stdcall C. fastcall D. naked
问题2：地址004010b0处的指令add esp,0Ch所代表的含义是什么？(3分)

综合题10分*3

- 2、给定8250,8254,8259格式, ICW1~4 OCW1~3 完成例题8.9 9.6
- 3、例8.6 8250地址范围为03F8H～03FFH，试编写程序设置发送字符长度为8位，2位停止位，偶校验。
  - 解答：线路控制寄存器的地址为3FBH（A2、A1、A0 = 011B），控制字应为00011111B。
  - 参考程序段如下：

```
MOV DX, 3FBH ;LCR地址
MOV AL, 00011111B ;
OUT DX, AL
```

7	6	5	4	3	2	1	0
DLAB	SB	SP	EPS	PEN	STB	WLS1	WLS

WLS1 WLS0	WLS1 WLS0＝00b，字符长度为 5 位；＝01b，字符长度为 6 位； ＝10b，字符长度为 7 位；＝11b，字符长度为 8 位
STB	＝0，停止位长度为 1 位；＝1、1.5 位或 2 位（字符长度为 5 位时，采用 1.5 位停位，字符长度为 6、7、8 位时，采用 2 位停止位）
PEN	＝0，不使用奇偶校验。发送接收时没有校验位
EPS	＝0，奇校验；　＝1，偶校验。EP＝0 时，此位无效
SP	＝1 时，奇偶校验位固定为 0 或 1；＝0 时，设置校验位
SB	＝1 时，发送线 SOUT 设为 0 并保持至少一个字符的时间，即产生一个间断，进发送间断状态；＝0 时，退出间断状态
DLAB	＝1，访问除数寄存器；DLAB＝0，访问其他寄存器

图 8－16　线路控制寄存器 LCR 的格式

编程题（15分）

- 2. 编写32位汇编语言程序，要求从键盘输入两个字符串，比较这两个字符串是否相同。若相同，则输出“Yes”，否则输出“No”。
- 要求：
- ①. 程序应有必要的注释（用中文说明）。
- ②. 程序应该是具有32位环境下控制台界面或者Windows界面的完整程序。

期待汇编接口课程后续的缘分...

的班主任是林勇钢老师。
CS的硕士，下个月就要毕
您教的，当时就非常喜欢
到在汶川大地震时，您的团
了一条求救微博并把这个消
命。

小的一个，但是却极大地影
为想要知道更多，想要能像
的时候，当我的导师Doug
挖掘这个方向，我就把您的
硕士求学经历中，我的导师
被这个小故事感动了，愿意

直关注您的微博，最近从您
前都拿到了特别棒的offer，
您分享我的好消息：我也是
me employment offer，职
，明年3月入职。入职后我
面的知识，一步一个脚印地

感谢关注聆听！

张华平
Email: kevinzhang@bit.edu.cn
微博：@ICTCLAS张华平博士
实验室官网：
http://www.nlpir.org

大数据千人会