汇编语言程序设计复习

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）
2016-12

期末考试：

- 中关村校区　COM07023　汇编语言程序设计
  张华平　计算机学院　48+10重考
  信4010　58　60　2017-01-16
  第24周 星期一 09:30~11:30 张华平
- 中关村校区　COM07023　汇编语言程序设计
  张华平　计算机学院　57　信5010
  57　60　2017-01-16　第25周
  星期一　09:30~11:30

地点：中教1013

复习范围：课件及教材相关内容

实验报告：各班学习委员收齐，Email给xiaguangmin2016@nlpir.org

总体目标：

运用汇编语言解决问题

- 能够把所学知识融会贯通，综合运用所学指令、伪指令、.EXE程序结构等知识，熟练地进行循环、分支、宏指令、子程序的设计工作。
- 熟练掌握上机步骤

第2章 汇编语言编程基础

复习重点：2.1、2.4、2.5

掌握：

- 汇编语言概念、优缺点、应用场合。
- 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。
- 存储器基本概念：字节、字、双字、存储顺序（逆序存放）等，存储器分段管理，实模式存储器寻址，20位物理地址的计算。
- 课后习题（ 2.17除外）

数据表示：01　FD(错误)→0FD

了解：2.2

第3章 PC指令系统

复习重点：

3.1、3.3、3.4.1、3.5.1、3.5.4、 3.5.5、3.6、3.7.1、3.8

掌握：

- 与数据有关的寻址方式：掌握各种寻址方式的表示、物理地址的计算、段超越前缀概念、灵活运用各种寻址方式编程。
- 指令系统：掌握基本指令集中的指令格式、功能、特殊要求（执行条件及结果）等，达到正确使用指令编写程序。
- 注意复习指令的程序片段示例及相关习题

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、ADC、INC、SUB、SBB、DEC、CMP、MUL、IMUL SRC、DIV、IDIV

3. 十进制运算指令基本概念：可参与运算的操作数，与二进制指令的关系

4. 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）、循环指令(LOOP：短转、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 汇编语言程序组织与开发环境

复习重点：

4.1~4.5、4.6.2、4.9、4.10

注意复习课后习题的4.1~4.16，完整程序及调试

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

汇编语言程序组织与开发环境（续）

掌握：

① 熟练掌握数据定义、符号定义、结构定义预置存取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（INT 21H的1、2、9、0AH功能，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

第5章　分支与循环程序设计

复习重点：

通过复习本章程序（例5.8、5.11除外），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6章　子程序设计

复习范围：课件及教材相关内容

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。

了解：缓冲区溢出攻击原理、6.7节

第8章　高级汇编语言技术

复习范围：课件（第7章）及教材（第8章）相关内容（8.1、8.2.1（1））

重点：

1. 掌握宏定义、调用方法，熟悉宏展开概念
2. 灵活使用宏指令编程（宏操作符不做要求）
3. 掌握宏指令库的设计及装入
4. 掌握本章所涉及到的伪指令的格式、功能、应用：MACRO/ENDM、LOCAL、PURGE、INCLUDE、REPT。
5. 掌握宏指令与子程序的区别。

了解：重复定义伪指令。

考试题型范围

1、选择 10*1

2、填空 20*1

3、程序填空题 20

4、读反汇编码回答问题：10

5、简答题（共25分）

6、编写程序 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

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。

指令改错（每道题2分，共10分，将错误原因直接写在题后）

- 1. MOV AL，DX

_____

_____

- 2. ADD [ESI]，VAR

_____

_____

四、程序填空题（每道题2分，共10分

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
```

五、读程序回答问题（共10分）

- 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)

六、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]

七、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。

表扬与自我表扬

汇编课延伸的缘分…

张老师，您好！

我是北理CS 09级4班的一名学生，我们的班主任是林勇钢老师。我2013年毕业以后来美国西北大学读了CS的硕士，下个月就要毕业了。我们大三时候的汇编这门课就是您教的，当时就非常喜欢您。您在课堂上曾经讲了一个故事，谈到在汶川大地震时，您的团队通过对微博平台的数据挖掘及时发现了一条求救微博并把这个消息迅速扩散了出去，拯救了被困者的生命。

其实这个故事只是您许多科研成果中极小的一个，但是却极大地影响了我后来的学生生涯和职业生涯。因为想要知道更多，想要能像您一样做这样酷酷的事，在我刚到美国的时候，当我的导师Doug Downey教授问我为什么一定要学数据挖掘这个方向，我就把您的这个小故事讲给他听。在我后来的整个硕士求学经历中，我的导师给了我很多的指导和支持，他说因为他被这个小故事感动了，愿意帮助我实现梦想。

我从本科大三上了您的汇编课开始就一直关注您的微博，最近从您的微博上得知您实验室的同学在毕业之前都拿到了特别棒的offer，

谢谢大家！

张华平
Email: kevinzhang@bit.edu.cn
微博：@ICTCLAS张华平博士
微信：drkevinzhang
欢迎大家访问大数据搜索与挖掘实验室官网：http://www.nlpir.org