## 汇编语言（王爽）

1. 寄存器

1.1通用寄存器

AX,BX,CX,DX

可分为AH(高字节),AL(低字节)

1.2段寄存器

CS:IP下一条指令地址  
DS存放段地址

1. 汇编指令

mov ,

add ,

Sub ,

1. 实验基础

Debug R,D,E,U,T,A（需加地址）

1. 栈

PUSH入栈

POP出栈

ss:sp

5.debug

D，E，A，T，

6.伪指令

a.段名 segment

段名 ends

b.end除了结束作用，还通知编译器程序入口在什么地方。如end start

c.assume

d.标号

7.[BX]偏移寄存器

8.loop指令

第一步：CX减一

第二步：判断CX

9.汇编源程序中，数据不能以字母开头

MOV ax,0ffffh

10.返回DOS环境

mov ax，4c00h

int 21h

11.使用数据定义

dw 后接数据

define word定义字型数据

dw 0用于申请空间

db 字符或字符串

dd双字型

dup用于数据的重复

db 3 dup (0)

12.and和or命令

13.汇编大小写字母转换

大写字母第五位为0，小写为1

14.偏移寄存器

SI源变址寄存器

DI目的变址寄存器

可以与BX和BP搭配来寻址

只有bx, si, di, bp可以做偏移，且bp默认ss

15.命令处理数据长度

a.寄存器指明

b.word ptr直接指明

byte ptr

c.指令默认

push只字操作

16.除法div和乘法mul

被除数16位 AX

32位 AX（低位）DX（高位）

高的商 低的余数

转移指令

17.offset

取得标号地址

mov ax，offset start

18.jmp指令

a.jmp short s段内短位移，指到标号位置

b.jmp far ptr s 段间转移，远转移

c.jmp 寄存器 直接修改ip指针

d.jmp 访问内存的方法

jmp word/dword ptr 内存地址

19.jcxz指令

条件转移指令

1. ret和retf

ret近转移 pop ip

retf远转移 pop ip,pop cs

1. call指令

Call 标号(段内) push ip jmp

Call for ptr 标号 push cs push ip jmp

Call 寄存器 push ip jmp

Call word/dword ptr 内存地址 push 地址 jmp

Call 和 ret可利用栈来控制子程序段

Call.....ret......

1. 寄存器冲突

比如cx，在子程序中将需要的寄存器压入栈，结束时再取出

1. 标志寄存器

ZF 零标志位

PF 奇偶标志位 所有的bit位上1的个数是否为偶数，偶pf=1

SF 符号标志位 负数sf=1

CF 无符号数进位/借位标志位

OF 有符号数溢出标志位

DF 串处理指令，控制si,di的增减

Df=0,每次操作后si,di递增

Df=1,每次操作后si,di递减

1. 带进位加法和减法：

abc:ax=ax+bx+cf

sbb:ax=ax-bx-cf

1. cmp指令

不计算结果，但是影响标志位

1. 条件转移指令

Je(equal)

Jne

Jb(below)

Jnb

Ja(above)

Jna

1. Movsb(move string byte)指令 串传送指令

Move es:di,ds:si

然后按照df标志进行自增、自减

Movsw(move string word)同上

搭配：rep movsb 利用cx重复做串复制

1. pushf和popf

pushf将标志寄存器的值压栈

Popf将标志寄存器的值出栈

1. 中断过程

①取得中断类型码

②pushf

③TF=0,IF=0

④push CS

⑤push IP

⑥改变CS:IP

1. 中断处理程序（类似子程序）和iret

①保存要用的寄存器

②处理中断

③恢复寄存器

④iret返回

Iret：pop ip

Pop cs

Popf

注意：字符串要存放在中断处理程序中

TF=1会触发单步中断，为避免循环中断，所以设置TF为0

1. 端口

In ax/al,60H(端口号)

Out 60h,ax/al

1. 移位指令

Shl 左移，最后移出的一位写入CF,z最低位0补齐

Slr 右移，。。。。。。。。。。。。。。。。。。。。。。。。。。。

小贴士：BCD码+30h=十进制对应的ascll码

1. 外中断：①不可屏蔽中断（少）

②可屏蔽中断

IF=1,立即响应

IF=0,先屏蔽，后来响应

注意：seg 取得某一标号的段地址

1. 偏移表

table db/dw ①字符表 ②调用子程序