1. 32 位间接寻址方式

(1) 32 位比 16 位多了以下这种寻址方式:

[寄存器+寄存器*n+常数]

其中 n=2、4、8。

例如:

```
mov eax, [ebx+esi*4+6]
```

VC 里面要查看当前 C 代码对应的机器语言，可以在按 F10 开始调试后选菜单:

```
View->Debug Windows->Disassembly
```

TC 里面要查看当前 C 代码对应的机器语言:

先把 ary.c(http://10.71.45.100/bhh/ary.c)拷到 dosbox86\tc,

集成环境中选菜单 File->Dos Shell->

```
cd \tc
tc
File->Load->ary.c
Compile->Compile
Compile->Link
File->Quit
td ary.exe
View->CPU
```

这种寻址方式的应用:

```
long a[10]={...};
int i, n=10, sum=0;
for(i=0; i<n; i++)
   sum += a[i];
```

设 ebx=&a[0], esi=0, eax=0, 则上述 C 代码可转化

成以下汇编代码：

```
again:
add eax, [ebx+esi*4]
add esi, 1
cmp esi, 10
jb again
```

(2) 32 位寻址方式里面，对[]中的两个寄存器几乎不加限制
例如：

ebx, ebp, esi, edi,
eax, ecx, edx, esp 都可以放到[]里面；
mov eax, [ebx+ebx*4]; 两个寄存器可以任意组合

2. 段跨越(segment overriding)

通过在操作数前添加一个段前缀(segment prefix)如 CS:、DS:、ES:、SS:来强制改变操作数的段址，这就是段跨越。

段地址的隐含：

```
mov ax, [bx]
mov ax, [si]
mov ax, [di+2]
mov ax, [bx+si]
mov ax, [bx+di+2]
mov ax, [1000h]
```

上述指令的源操作数都省略了段地址 ds。

[bp], [bp+2], [bp+si+2], [bp+di-1]
等价于
ss:[bp], ss:[bp+2], ss:[bp+si+2], ss:[bp+di-1]
当[]中包含有寄存器 bp 时，该变量的段地址一定是 ss。
例如：
mov ax, [bp+2] 相当于

```
mov ax, ss:[bp+2]
```

默认的段地址是可以改变的，例如：

```
mov ax, ds:[bp+2]
```

这条指令的源操作数段地址从默认的 ss 改成了 ds。

同理，

`mov ax, [bx+si+2]`改成`mov ax, ss:[bx+si+2]`的话，默认段地址就从 ds 变成了 ss。

3．通用数据传送指令：MOV，PUSH，POP，XCHG

```
mov byte ptr ds:[bx], byte ptr es:[di]
```

错误原因:两个操作数不能同时为内存变量

以下为正确写法：

```
mov al, es:[di]
mov ds:[bx], al
```

32 位 push、pop 过程演示：

http://10.71.45.100/bhh/stk1.txt 代码

http://10.71.45.100/bhh/stk2.txt 堆栈布局

push/pop 后面也可以跟变量,例如：

```
push word ptr ds:[bx+2]
pop word ptr es:[di]
```

8086 中，push 不能跟常数，但 80386 及以后的 cpu 允许 push 一个常数。

push/pop 后面不能跟一个 8 位的寄存器或变量。

```
mov ax, 1
mov bx, 2
xchg ax, bx; 则 ax=2, bx=1
```

4. 除法指令: div

(1) 16 位除以 8 位得 8 位

ax / 除数 = AL..AH

例如: div bh

设 AX=123h, BH=10h

```
div bh; AL=12h, AH=03h
```

(2) 32 位除以 16 位得 16 位

dx:ax / 除数 = ax..dx

例如: div bx

设 dx=123h, ax=4567h, bx=1000h

```
div bx ; 1234567h/1000h
       ; AX=1234h, DX=0567h
```

(3) 64 位除以 32 位得 32 位

edx:eax / 除数 = eax..edx

例如: div ebx

假定要把一个 32 位整数如 7FFFFFFFh 转化成十进制格式

则一定要采用(3)这种除法以防止发生除法溢出。

代码: http://10.71.45.100/bhh/val2decy.asm

5. 地址传送指令: LEA, LDS, LES

(1) lea dest, src

```
lea dx, ds:[1000h] ; DX=1000h
mov dx, 1000h; 上述 lea 指令的效果等同于 mov 指令

lea dx, abc ; 效果等价于以下指令
mov dx, offset abc

lea dx, ds:[bx+si+3]; dx=bx+si+3
mov dx, bx+si+3; 错误
mov dx, bx; \
add dx, si;  | 效果等同于上述 lea 指令
add dx, 3 ; /

lea eax, [eax+4*eax]; EAX=EAX*5 用 lea 做乘法
lea eax, [eax+eax*2]; EAX=EAX*3
```

(2) 远指针(far pointer)

16 位汇编中，远指针是指 16 位段地址+16 位偏移地址；
32 位汇编中，远指针是指 16 位段地址+32 位偏移地址。
近指针(near pointer):
16 位汇编中，近指针是指 16 位的偏移地址；
32 位汇编中，近指针是指 32 位的偏移地址；

远指针(far pointer)包括段地址及偏移地址两个部分；
近指针(near pointer)只包括偏移地址，不包含段地址。

假定把一个远指针 1234:5678 存放到地址 1000:0000 中，则内存布局如下：

```
1000:0000 78h
1000:0001 56h
```

```
1000:0002 34h
1000:0003 12h
```

假定要把 1000:0000 中存放的远指针取出来，存放到 es:bx 中，则

```
mov ax, 1000h
mov ds, ax
les bx, dword ptr ds:[0000h]
          ; es=1234h, bx=5678h
```

远指针的汇编语言例子：

http://10.71.45.100/bhh/les.asm

近指针的汇编语言例子：

http://10.71.45.100/bhh/nearptr.asm

远指针的 C 语言例子：

http://10.71.45.100/bhh/farptr.c