8086指令

指令系统

计算机的指令系统是指该计算机能够执行的全部指令的集合，每种计算机都有它支持的指令集合。

16位8086指令系统是Intel 80x86系列微处理器指令系统的基础。

汇编调试器Debug

名称	解释	格式
a(Assemble)	逐行汇编	a [address]
c(Compare)	比较两内存块	c range address
d(Dump)	内存16进制显示	d [address]或 d [range]
e(Enter)	修改内存字节	e address [list]
f(fin)	预置一段内存	f range list
g(Go)	执行程序	g [=address] [address...]
h(Hexavithmetic)	进制算术运算	h value value
i(Input)	从指定端口地址输入	i pataddress
l(Load)	读盘	l [address [driver seetor]]
m(Move)	内存块传送	m range address
n(Name)	置文件名	n filespec [filespec...]
o(Output)	从指定端口地址输出	o portadress byte
p	执行循环、重复的字符串指令、软件中断或子例程。不跟踪内部。	p
q(Quit)	结束	q
r(Register)	显示和修改寄存器	r [register name]
s(Search)	查找字节串	s range list
t(Trace)	跟踪执行	t [=address] [value]
u(Unassemble)	反汇编	u [address]或range
w(Write)	存盘	w [address[driver sector secnum]]

寄存器

寄存器是CPU中程序员可以用执行读写的部件。程序员通过改变各种寄存器中的内容来实现对CPU的控制

1. 通用寄存器

	高低位	名称
AX	AH,AL	累加寄存器(Add)
BX	BH,BL	基址寄存器(Base)
CX	CH,CL	计数寄存器(Count)
DX	DH,CL	数据寄存器(Data)
BP		基址指针寄存器(Base Point)
SP		堆栈指针寄存器(Stack Point)
SI		源变址寄存器(Source)
DI		目的变址寄存器(Destination)

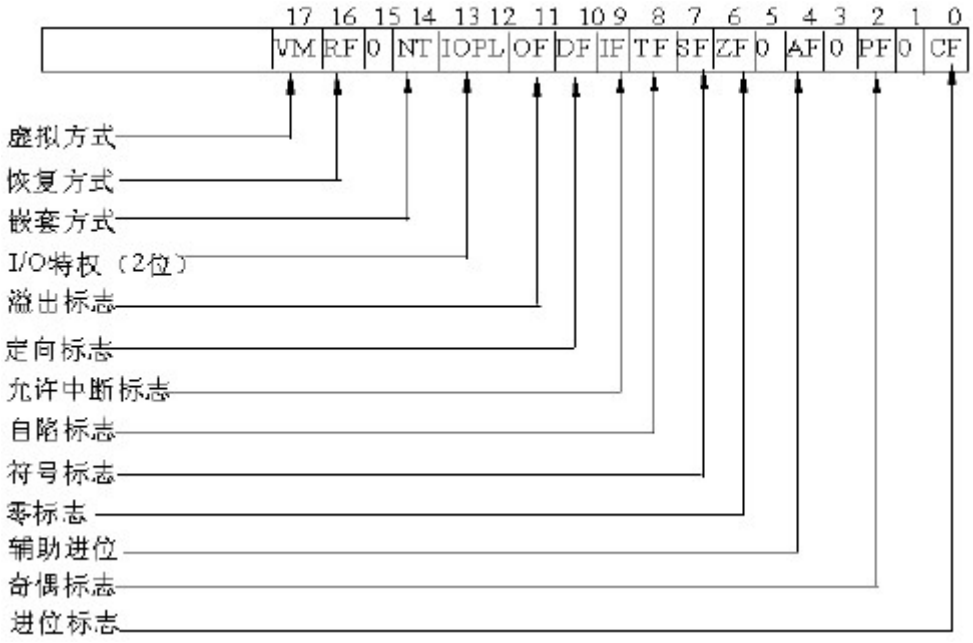
2. 指令指针寄存器

	名称
IP	指令指针寄存器

3. 标志寄存器

（1）用来存储相关指令的某些执行结果。
（2）用来为CPU执行相关指令提供行为依据。
（3）用来控制CPU的相关工作方式。

	名称
Flags	标志寄存器



标志位（外语缩写）	标志位名称及外语全称	= 1	= 0
CF	进位标志/Carry Flag	CY/Carry/进位	NC/No Carry/无进位
PF	奇偶标志/Parity Flag	PE/Parity Even/偶	PO/Parity Odd/奇
AF	辅助进位标志/Auxiliary Carry Flag	AC/Auxiliary Carry/进位	NA/No Auxiliary Carry/无进位
ZF	零标志/Zero Flag	ZR/Zero/等于零	NZ/Not Zero/不等于零
SF	符号标志/Sign Flag	NG/Negative/负	PL/Positive/非负
TF	跟踪标志/Trace Flag		
IF	中断标志/Interrupt Flag	EI/Enable Interrupt/允许	DI/Disable Interrupt/禁止
DF	方向标志/Direction Flag	DN/Down/减少	UP/增加
OF	溢出标志/Overflow Flag	OV/Overflow/溢出	NV/Not Overflow/未溢出

4. 段寄存器

	名称	说明
CS	代码段寄存器(Code Segment)	存放当前正在运行的程序代码所在段的段基址，表示当前使用的指令代码可以从该段寄存器指定的存储器段中取得，相应的偏移量则由IP提供。
DS	数据段寄存器(Data Segment)	指出当前程序使用的数据所存放段的最低地址，即存放数据段的段基址。
SS	堆栈段寄存器(Stack Segment)	指出当前堆栈的底部地址，即存放堆栈段的段基址。
ES	附加段寄存器(Extra Segment)	指出当前程序使用附加数据段的段基址，该段是串操作指令中目的串所在的段。

段寄存器超越前缀与使用规定

- 超越前缀

  没有指明时，一般的数据访问在DS段；使用BP访问主存，则在SS段。默认的情况允许改变，需要使用段超越前缀指令，8086指令系统中有4个

CS:	代码段超越，使用代码段的数据
SS:	堆栈段超越，使用堆栈段的数据
DS:	数据段超越，使用数据段的数据
ES:	附加段超越，使用附加段的数据

- 使用规定

访问存储器的方式	默认	可超越	偏移地址
取指令	CS	无	IP
堆栈操作	SS	无	SP
一般数据访问	DS	CS ES SS	有效地址EA
BP基址的寻址方式	SS	CS ES DS	有效地址EA
串操作的源操作数	DS	CS ES SS	SI
串操作的目的操作数	ES	无	DI

数据的存储

单位

- 二进制位`Bit`：存储一位二进制数
- 字节`Byte`：8个二进制位，D7～D0
- 字`Word`：16位，2个字节，D15～D0

- 双字`DWord`：32位，4个字节，D31～D0
- 最低有效位`LSB`：数据的最低位，D0位
- 最高有效位`MSB`：数据的最高位，对应字节、字、双字分别指D7、D15、D31位

存储

80x86处理器采用**低位在低地址上，高位在高地址上**的存储形式，被称为小尾方式`Little Endian`。

```
0x12345678 ---> 0x78 0x65 0x34 0x12
              低地址     --->     高地址
```

而低位在高地址上，高位在低地址上的存储形式，被称为大尾方式`Big Endian`。

```
0x12345678 ---> 0x12 0x34 0x56 0x78
              低地址     --->     高地址
```

分段

8086CPU有20位的总线，寻址空间为2^20 = 1MB，即`0x00000～0xFFFFF`

8086CPU将1MB空间分成许多逻辑段

- 每个段最大限制为64KB
- 段地址的低4位为`0000`

表示形式为：**段基址 ： 段内偏移**

寻址方式为：**段基址*16+偏移地址=物理地址**，即CPU在访问内存时，用一个基础地址（段地址*16）和一个相对于基础地址的偏移地址相加，给出内存单元的物理地址

故，1MB的空间最多可以有：`2^20 / 16 = 2^16 =64K`个段，最少有：`2^20 / 2^16 = 16`个段