Assembly Programming

第六周 寻址方式

庞彦

yanpang@gzhu.edu.cn

Fall 2023

80X86的寻址方式

- 寻址的概念
- 与数据有关的寻址方式
  - 立即寻址
  - 寄存器寻址
  - 直接寻址
  - 寄存器间接寻址
  - 寄存器相对寻址
  - 基址变址寻址
  - 相对基址变址寻址

80X86的寻址方式

- 寻址的概念
- 与数据有关的寻址方式

  - 立即寻址
  - 寄存器寻址
  - 直接寻址
  - 寄存器间接寻址
  - 寄存器相对寻址
  - 基址变址寻址
  - 相对基址变址寻址

寻址的概念

汇编指令格式：
操作码　［操作数1［,操作数2［,操作数3]]]　［;注释］

寻址、寻址方式的概念：

- 寻址就是寻找操作数的地址。
- 寻址方式就是寻找操作数地址的方法。

寻址的目的：指令指定操作数的位置，即给出地址信息，在执行时需要根据这个地址信息找到需要的操作数。

寻址的概念

操作数有三种来源：

① 操作数在指令中，称立即数操作数

如　MOV AL，9

② 操作数在寄存器中，称寄存器操作数

指令中给出用符号表示的寄存器名。

如　MOV AL，BL

③ 操作数在内存单元中，称存储器操作数或内存操作数

指令中给出该内存单元的地址。用[　]表示存储器操作数

如　MOV AL，[2000H]

寻址方式分类：

1)**与数据有关的寻址方式**：确定内存单元的地址

2)与转移地址有关的寻址方式：确定转移地址

80X86的寻址方式

- 寻址的概念
- 与数据有关的寻址方式

  - 立即寻址
  - 寄存器寻址
  - 直接寻址
  - 寄存器间接寻址
  - 寄存器相对寻址
  - 基址变址寻址
  - 相对基址变址寻址

与数据有关的寻址方式

以 MOV 指令为例:

- 立即寻址　　MOV AX , 3069H
- 寄存器寻址　　MOV AX , BX
- 直接寻址　　MOV AX , [2000H]
- 寄存器间接寻址　　MOV AX , [BX]
- 寄存器相对寻址　　MOV AX , COUNT [SI]
- 基址变址寻址　　MOV AX , [BP] [DI]
- 相对基址变址寻址　　MOV AX , MASK [BX] [SI]

与数据有关的寻址方式

1. 立即寻址方式

操作数直接存放在指令中，紧跟在操作码之后，作为指令的一部分，这种操作数称为立即数。

- 立即数可以是8位或16位(16位的立即数是高位字节放在高地址，低位字节放在低地址)。
- 应用场合：立即数常用来给寄存器或内存单元赋初值。

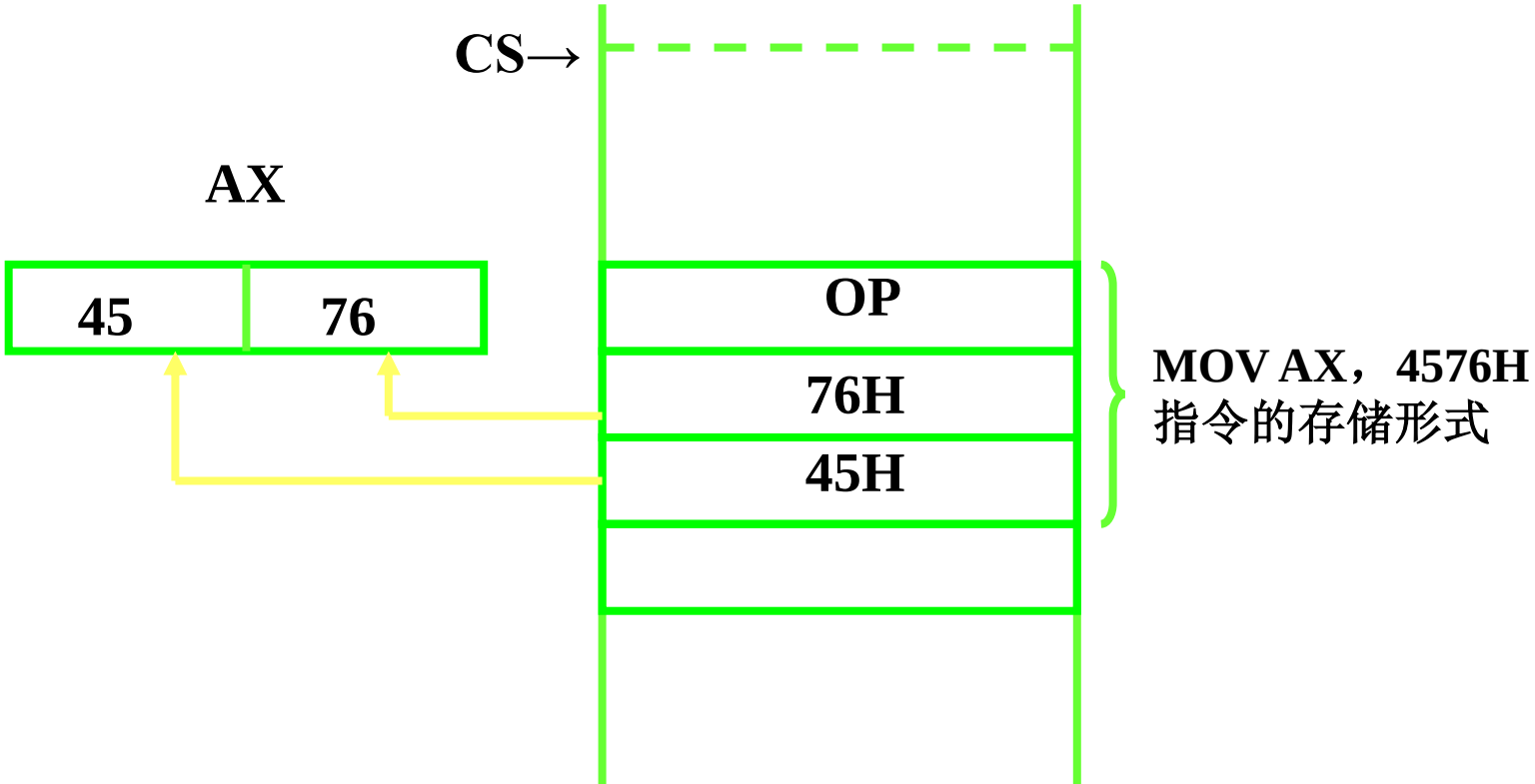
注意：只能用于源操作数字段，不能用于目的操作数字段。

与数据有关的寻址方式

【例】 MOV AX，4576H 执行后（AX）=?

该例中源操作数为立即寻址方式，立即数为4576H，存放在指令的下一单元。

执行：4576H→AX 执行后：（AX）=4576H

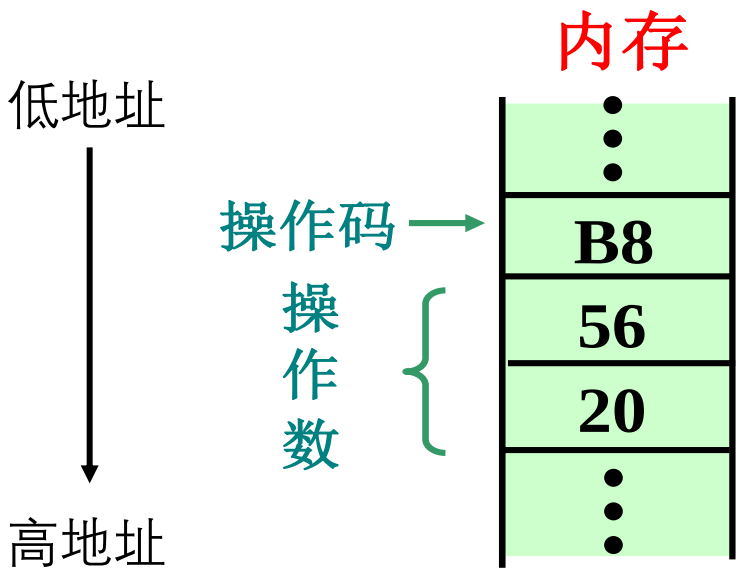


与数据有关的寻址方式

例　MOV　AX , 2056H

结果　(AH) = 20H

(AL) = 56H



例　MOV　78 H, AL　(right?)

与数据有关的寻址方式

2.寄存器寻址方式

定义：指令所要的操作数已存储在某寄存器中，或把目标操作数存入寄存器。

指令中可以引用的寄存器如下：

8位寄存器：AH、AL、BH、BL、CH、CL、DH、DL等；

16位寄存器：AX、BX、CX、DX、SI、DI、SP、BP和段寄存器等。

注：由于指令所需的操作数已存储在寄存器中，或操作的结果存入寄存器，这样，在指令执行过程中，会减少读/写存储器单元的次数，所以，使用寄存器寻址方式的指令具有较快的执行速度。通常情况下，提倡在编写汇编语言程序时，应尽可能地使用寄存器寻址方式。

与数据有关的寻址方式

【例】下列程序执行后，（AX）=？，（BX）=？

```
MOV  AX，1234H
MOV  BX，5678H
ADD  AX，BX
```

与数据有关的寻址方式

【例】下列程序执行后，（AX）=？，（BX）=？

```
MOV  AX，1234H
MOV  BX，5678H
ADD  AX，BX
```

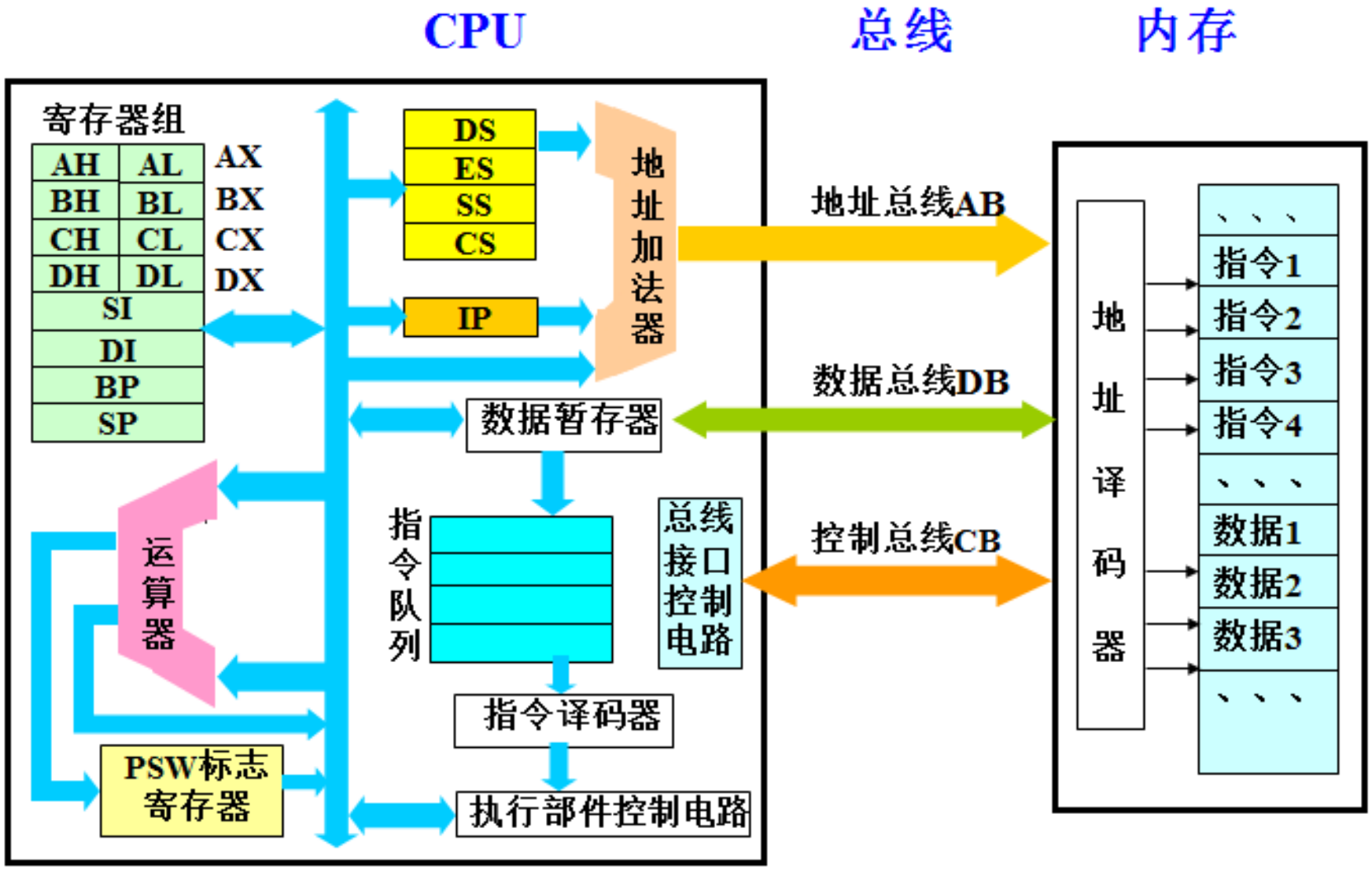
执行：1234H→AX

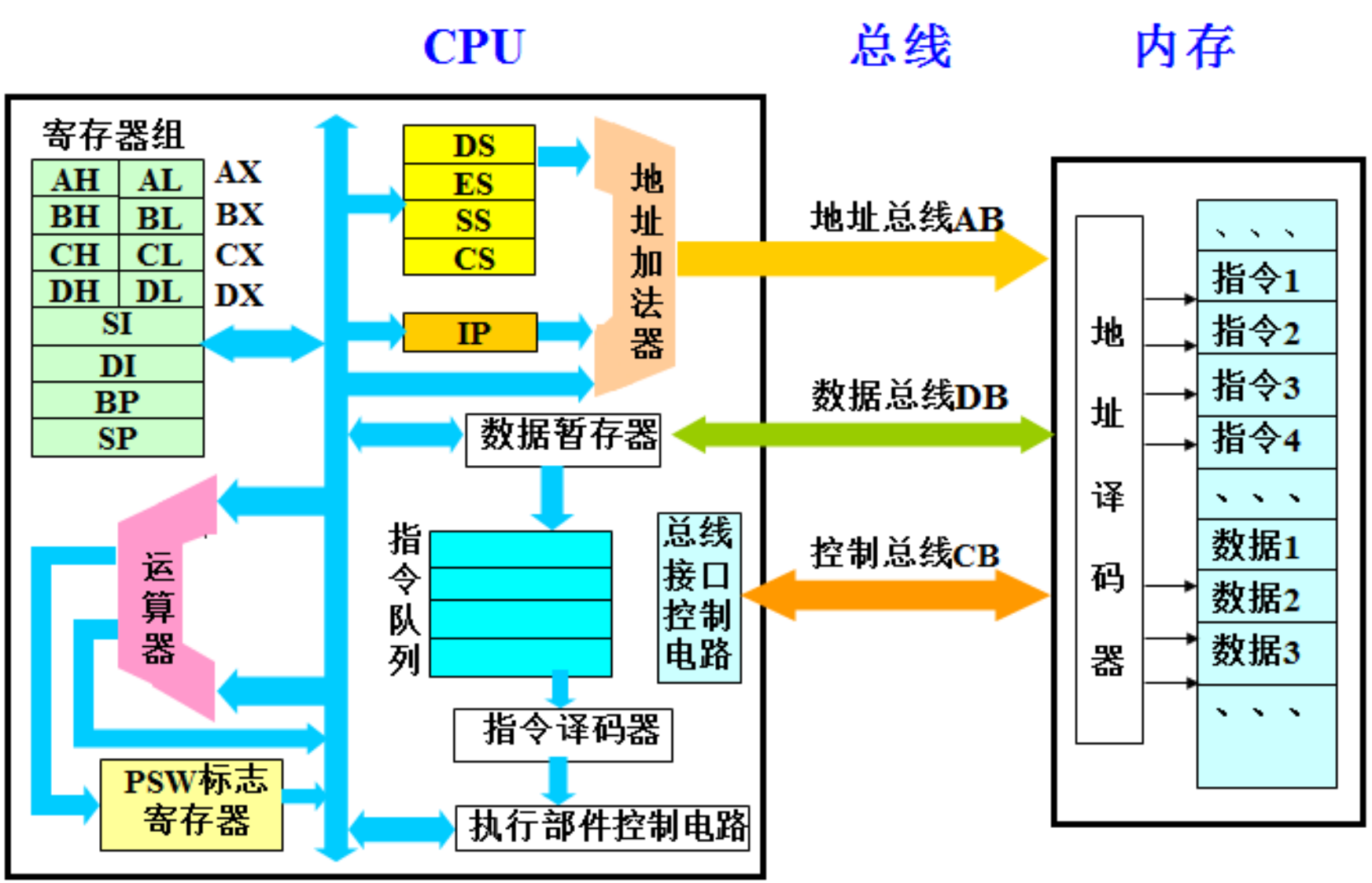
5678H→BX

“ADD AX，BX”：**（AX）+（BX）→AX**

执行后：（AX）=68ACH，（BX）=5678H

▲以上立即数寻址、寄存器寻址的操作数，
不用在取完指令后再到内存中取数。





▲以下 5 种寻址方式：

操作数存放在内存中，取完指令后，还需到内存取数。

指令中给出的是该操作数的地址，包括段地址和偏移地址。

与数据有关的寻址方式

3. 存储器寻址

除上述寻址方式外，以下各种寻址方式，操作数都在除代码段之外的存储区中。通过不同的寻址方式，获得操作数地址，从而取得操作数。

在前面的章节中，我们知道操作数的物理地址（Physical Address，PA）等于段基址左移4位，再加上偏移地址。

下面主要解决的问题是如何得到操作数的偏移地址。在8086/8088里，将操作数的偏移地址又称为有效地址（effective address，即EA），因此以下的各种寻址方式即为求有效地址（EA）的不同途径。

与数据有关的寻址方式

8086/8088指令中有效地址（EA）由以下3部分组成：

EA=基址＋变址＋位移量

①位移量（displacement）：存放在指令中的一个8位或16位的数，但它不是立即数，而是一个地址；

②基址（base）：存放在基址寄存器（BX、BP）中的内容。它是有效地址中的基址部分，通常用于指向数据段中数组或字符串的首地址。

③变址（index）：存放在变址寄存器（SI、DI）中的内容。通常用来指向数组中某个元素或字符串的某个字符。

根据有效地址中含有的成分不同，分别构成不同的寻址方式 。

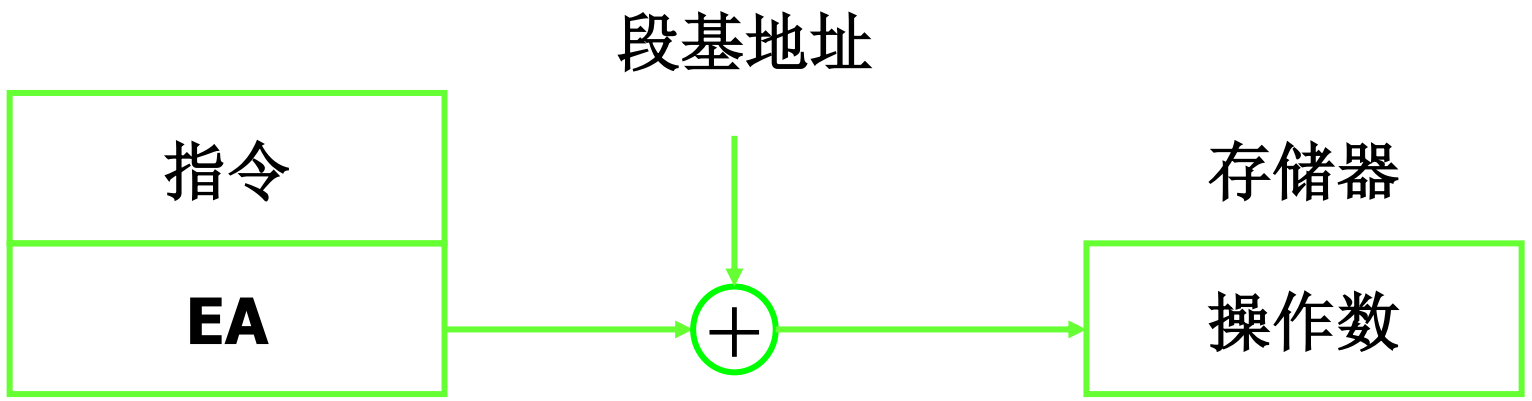
三种成分	16位寻址	32位寻址
位移量	0、8、16位	0、8、32位
基址寄存器	BX、BP	任何32位通用寄存器
变址寄存器	SI、DI	除ESP外的32位通用寄存器

与数据有关的寻址方式

(1) 直接寻址

定义：指令所要的操作数存放在内存中，在指令中直接给出该操作数的有效地址，这种寻址方式为直接寻址方式。

图形表示：



与数据有关的寻址方式

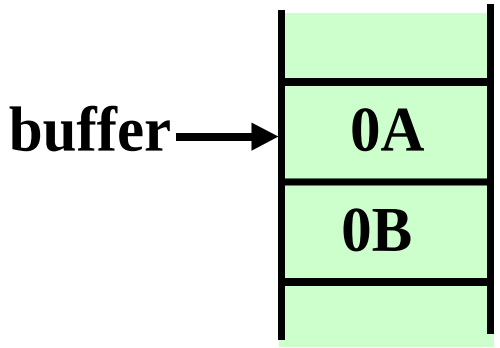
●在汇编语言程序中，一般不直接用数值表示偏移地址，而用符号代替数值表示地址，称符号地址(变量名)。

例　符号buffer表示一个地址。

MOV　AX , [buffer]

或写成　　MOV　AX , buffer

源操作数为buffer指向的内存单元的内容



符号地址(变量名)经汇编连接后，与一个确定的数值地址相对应。可用操作符Offset 获取变量的偏移地址。

故　PA = (DS)×10H + Offset　buffer

指令执行结果　(AX) = 0B0A H

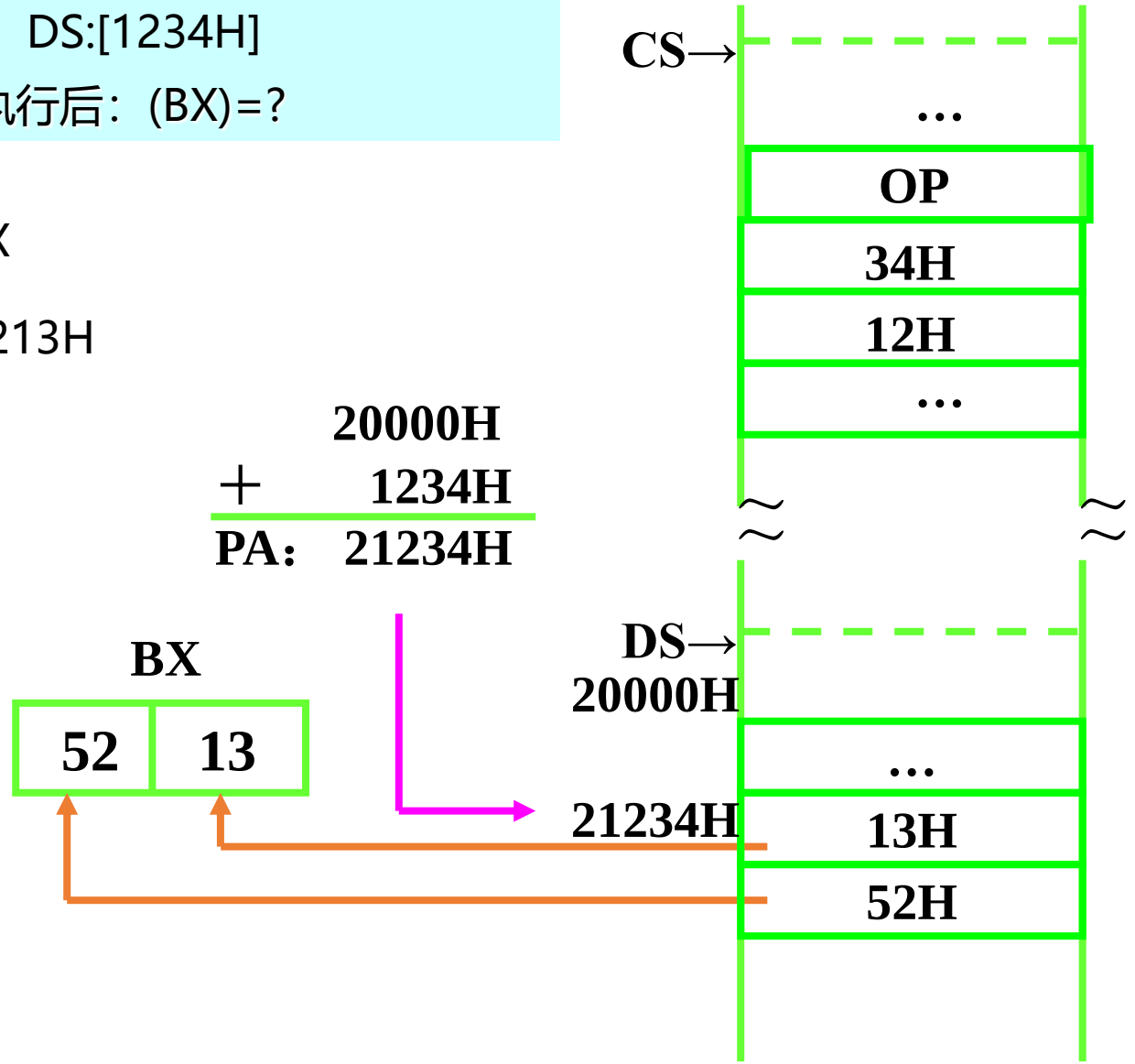
与数据有关的寻址方式

例：执行指令MOV BX，DS:[1234H]

设（DS）=2000H。执行后：(BX)=?

执行：（21234H）→BX

执行后：（BX）=5213H



与数据有关的寻址方式

例： MOV AX , DS:[1000 H]

若 (DS) = 2000H

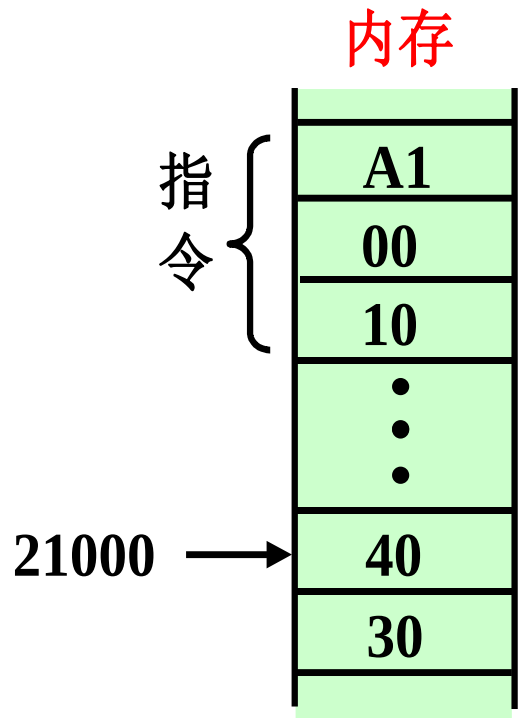
内存操作数的物理地址为：

PA = (DS)×10H +EA

=

=

执行后 (AX)=



与数据有关的寻址方式

例： MOV AX , DS:[1000 H]

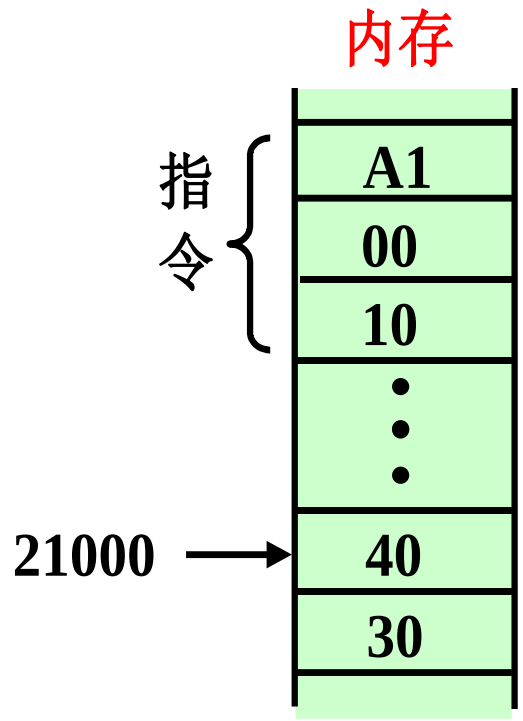
若 (DS) = 2000H

内存操作数的物理地址为：

PA = (DS)×10H +EA

= 2000H × 10H + 1000H

= 21000H



执行后 (AX)= 3040H

指令 MOV AX, [1000H] 与MOV AX, 1000H有什么不同?

指令 MOV AX, DS:[1000H] 与MOV AX, 1000H有什么不同?

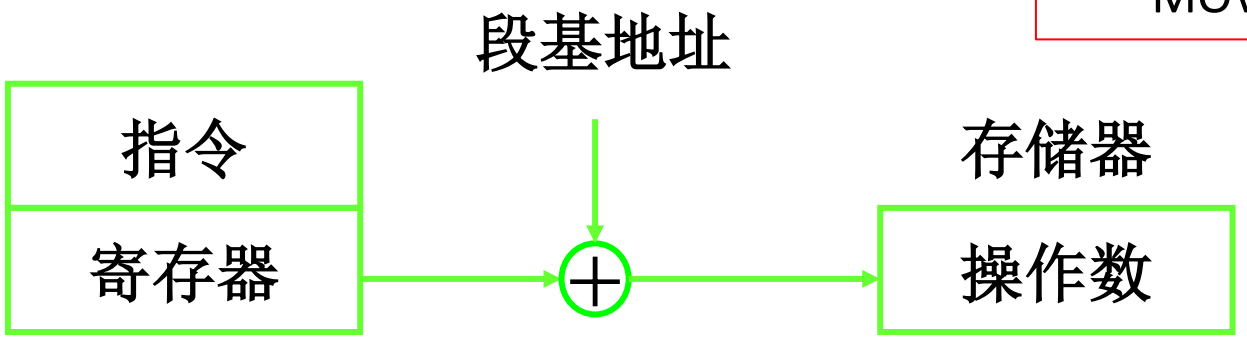
与数据有关的寻址方式

(2) 寄存器间接寻址

定义：操作数的有效地址只包含基址寄存器内容或变址寄存器内容一种成分。因此，有效地址就在某个存储器里，操作数的有效地址EA由寄存器给出。

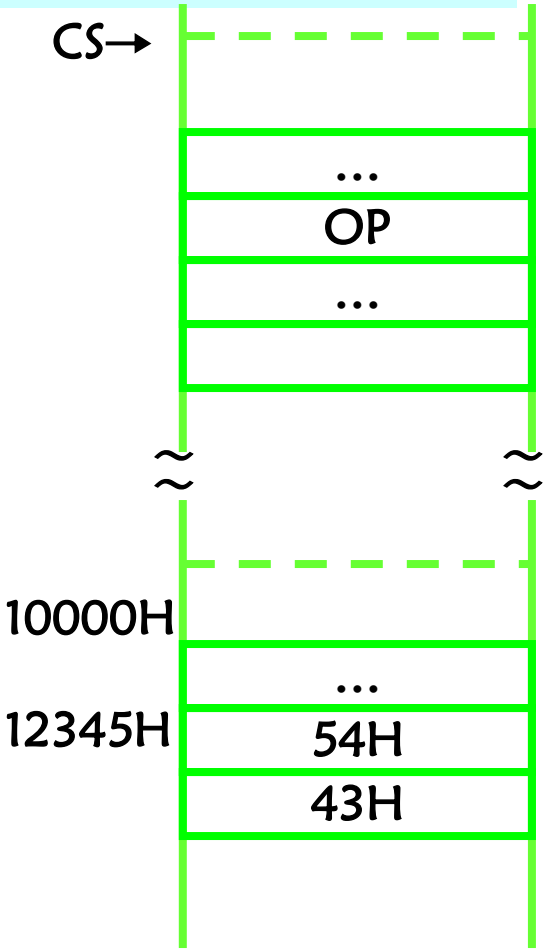
可用的寄存器有 BX 、 BP、 SI、 DI

```
如:  MOV   AL, [BX]
     MOV   DH, [BP]
     MOV   AH, [SI]
     MOV   DL, [DI]
```



与数据有关的寻址方式

【例3.4】假设有指令：MOV　　BX，[DI]，在执行时，（DS）=1000H，（DI）=2345H，存储单元（12345H）=4354H。问执行指令后，BX的值是什么?



与数据有关的寻址方式

【例3.4】假设有指令：MOV　　BX，[DI]，在执行时，（DS）=1000H，（DI）=2345H，存储单元（12345H）=4354H。问执行指令后，BX的值是什么?

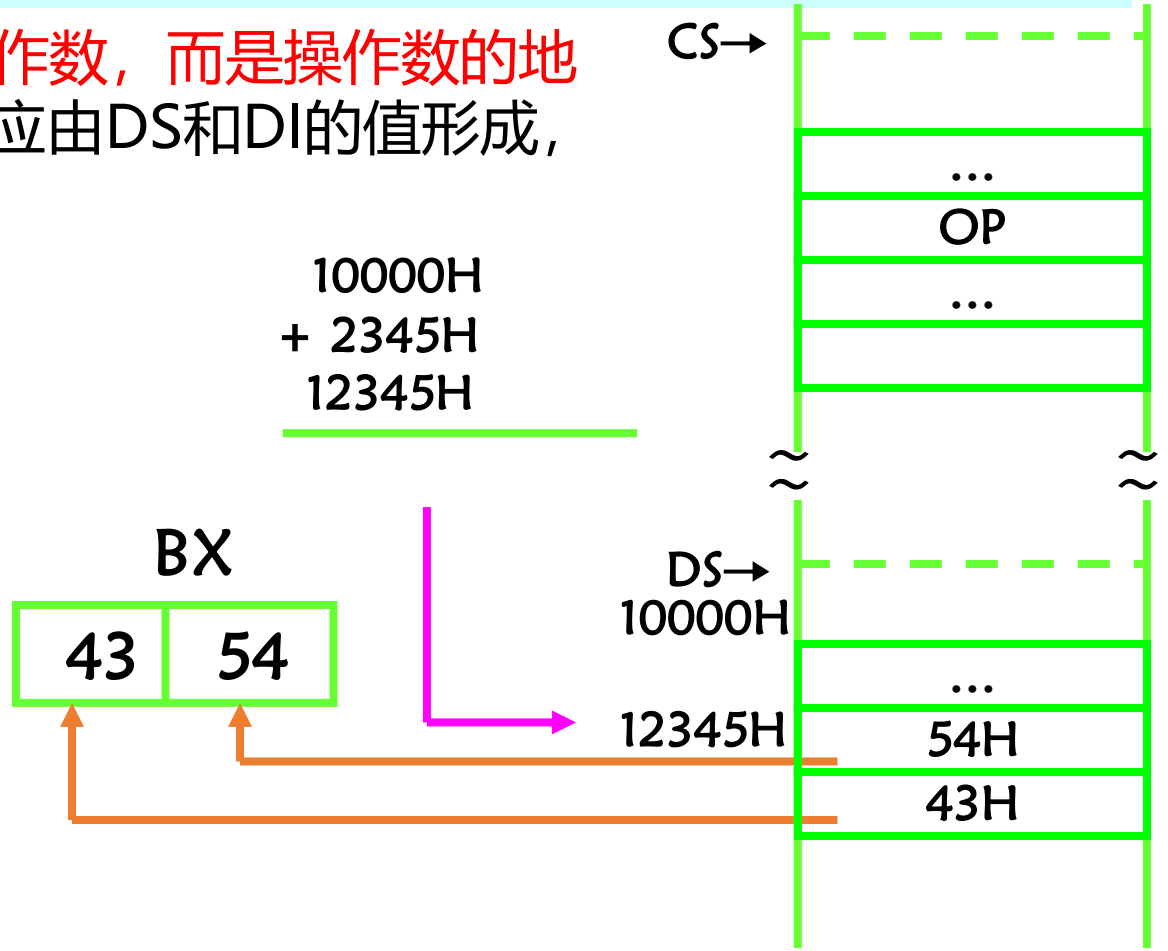
解：寄存器DI的值不是操作数，而是操作数的地址。该操作数的物理地址应由DS和DI的值形成，即：

PA=（DS）*16+DI

=1000H*16+2345H

=12345H。

该指令的执行效果是：把从物理地址为12345H开始的一个字的值传送给BX。

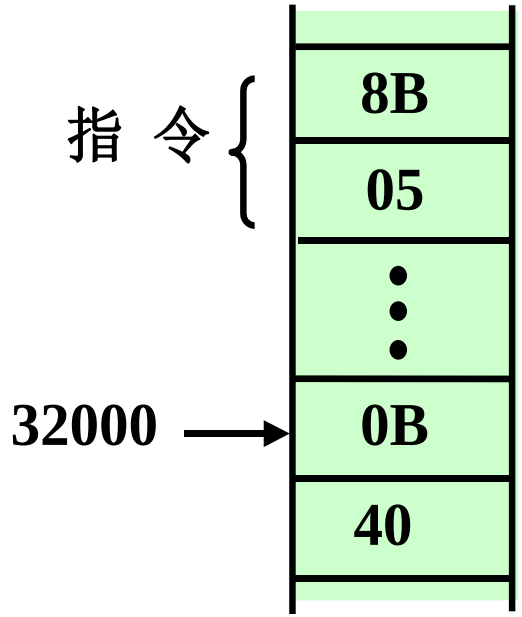


与数据有关的寻址方式

例： MOV AX , [DI]

若 (DS) = 3000H

(DI) = 2000H



(AX) = ?

思考： 指令 MOV AX,[DI] 与指令MOV AX, DI有什么不同?

与数据有关的寻址方式

例： MOV AX , [DI]

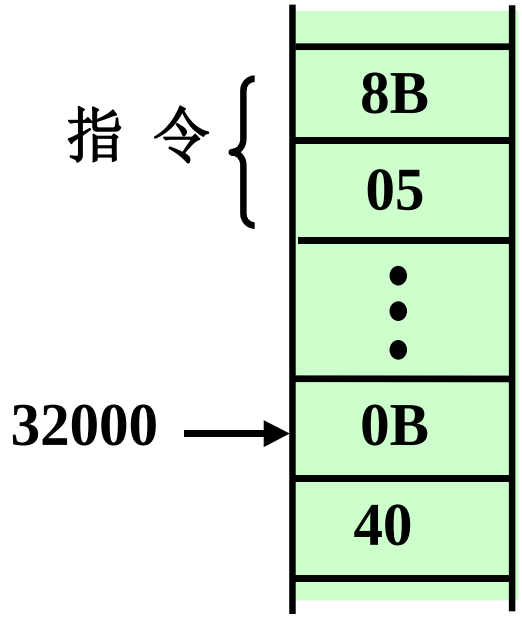
若 (DS) = 3000H

(DI) = 2000H

则内存操作数的物理地址为：

PA = (DS)×10H + (DI)

= 32000H



执行后 (AX) = (32000H) = 400BH

思考： 指令 MOV AX,[DI] 与指令MOV AX, DI有什么不同?

与数据有关的寻址方式

【例3.4】假设有指令：MOV　　BX，[DI]，在执行时，（DS）=1000H，（DI）=2345H，存储单元（12345H）=4354H。问执行指令后，BX的值是什么?

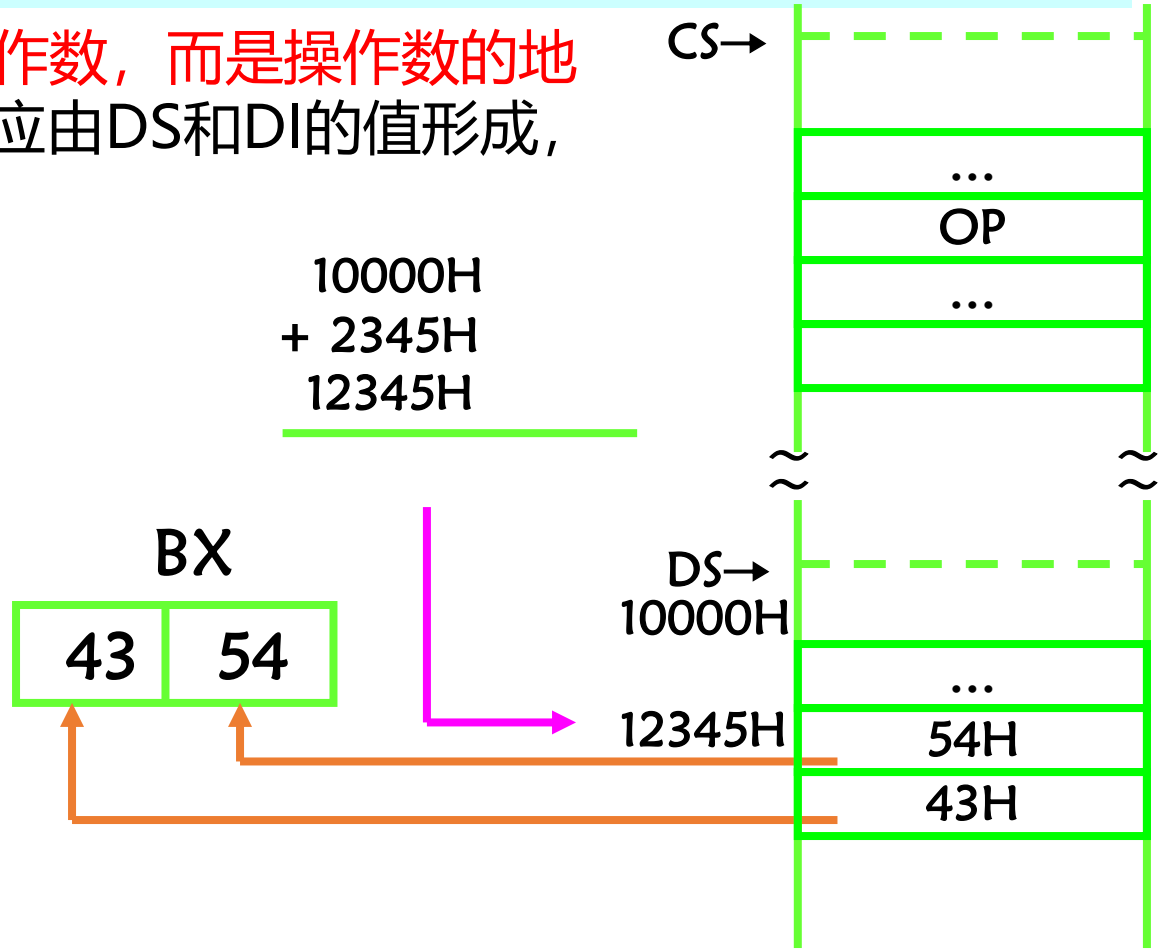
解：寄存器DI的值不是操作数，而是操作数的地址。该操作数的物理地址应由DS和DI的值形成，即：

PA=（DS）*16+DI

=1000H*16+2345H

=12345H。

该指令的执行效果是：把从物理地址为12345H开始的一个字的值传送给BX。



与数据有关的寻址方式

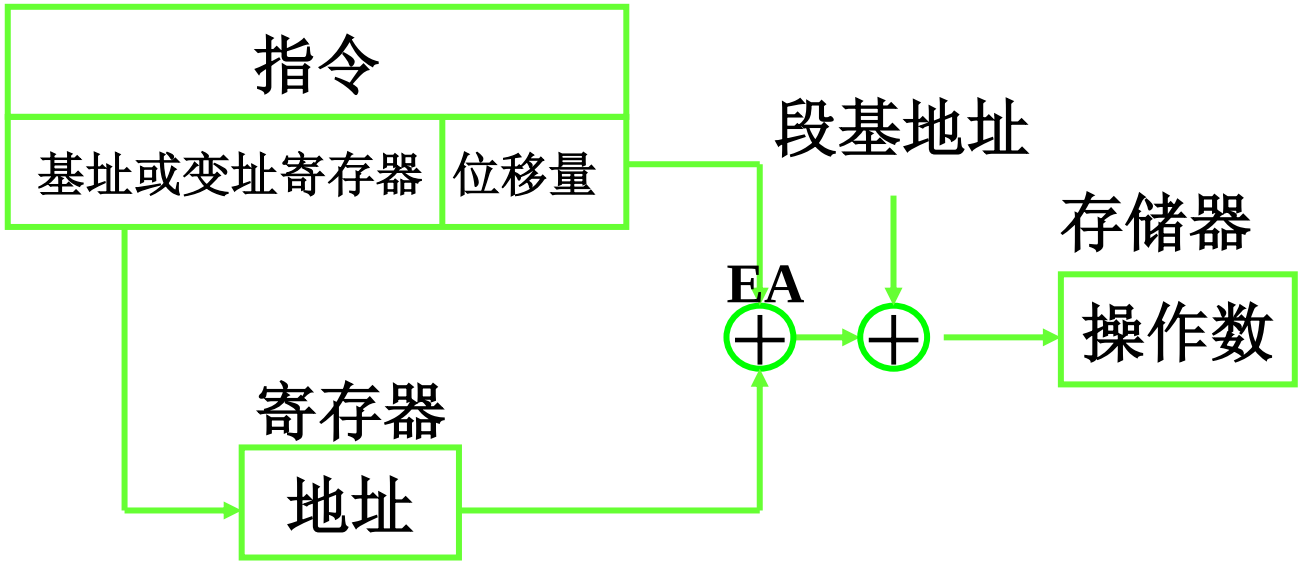
(3) 寄存器相对寻址方式

定义：操作数在存储器中，其有效地址是一个基址寄存器（BX、BP）或变址寄存器（SI、DI）的内容和指令中的8位/16位偏移量之和。使用BP时，其默认段是SS段，其他寄存器默认为DS段。

汇编格式：X[R]或[R+X]（X表示位移量，是8位或16位有符号数）

功能：操作数存放在存储器，寄存器R的内容加位移量X为操作数的偏移地址EA。

图形表示如右：



与数据有关的寻址方式

如:

```
MOV   AL,  [ BX +10H]
MOV   AH,  [ DI+20H ]
MOV   DL,  30H [ SI ]
MOV   DH,  40H [ BP ]
```

与数据有关的寻址方式

如:　　MOV　AL, [BX +10H]

MOV　AH, [DI+20H]

MOV　DL, 30H [SI]

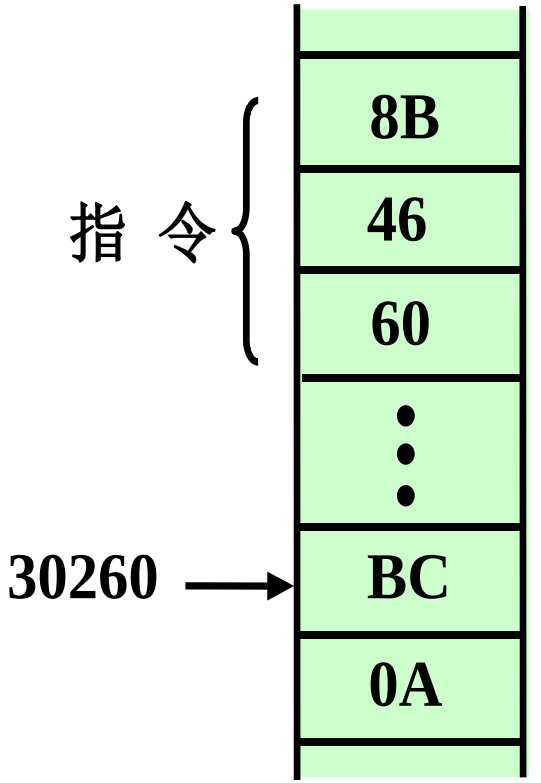
MOV　DH, 40H [BP]

例: MOV AX , 60H [BP]

若（DS）=2000H, （SS) = 3000H

(BP) = 200H

则内存操作数的物理地址为?



与数据有关的寻址方式

如:　　MOV　AL, [BX +10H]

　　MOV　AH, [DI+20H]

　　MOV　DL, 30H [SI]

　　MOV　DH, 40H [BP]

例: MOV AX , 60H [BP]

若（DS）=2000H, （SS）= 3000H

（BP）= 200H

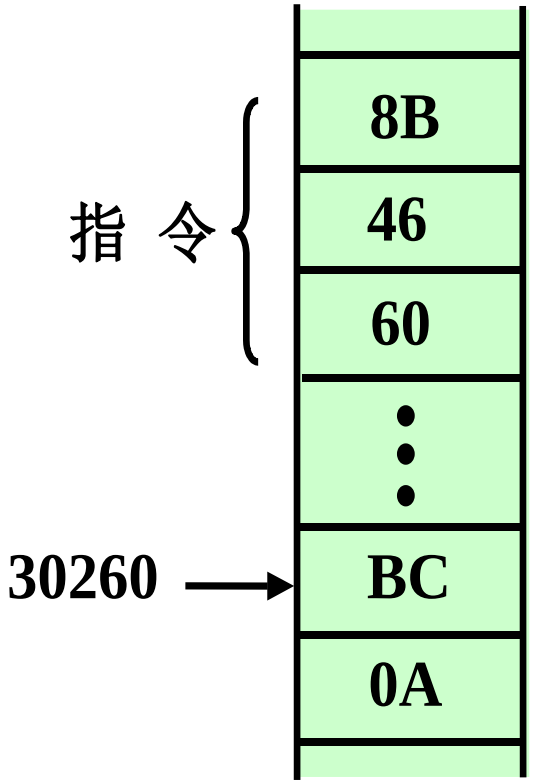
则内存操作数的物理地址为?

PA = (SS)×10H + (BP) + 60H

= 30260H

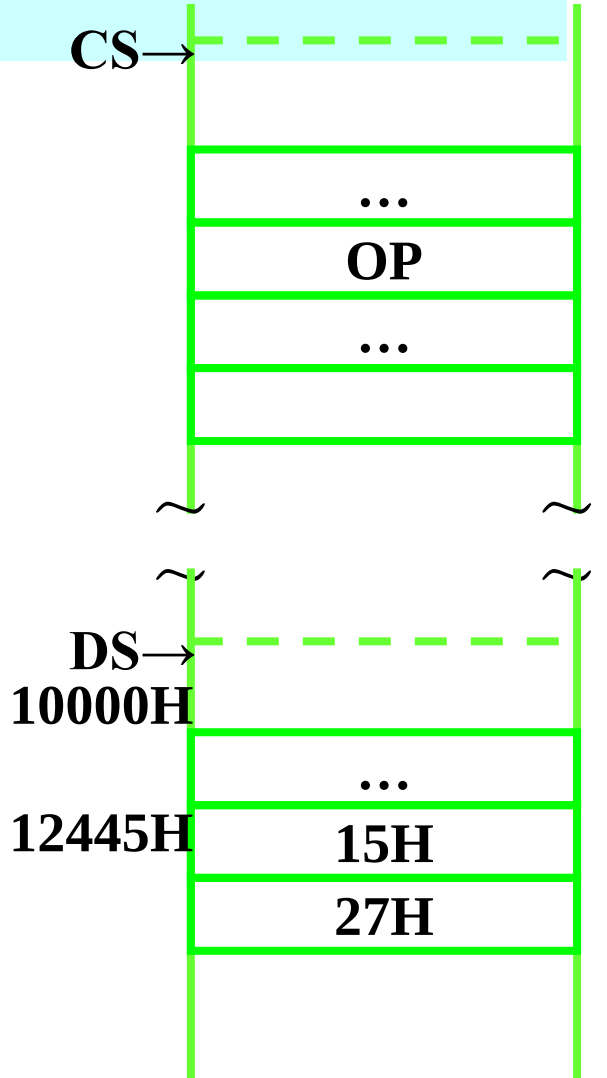
指令执行后:

(AX) = (30260H) = 0ABCH



与数据有关的寻址方式

【例3.5】假设指令：MOV BX, [SI+100H]，在执行它时，（DS）=1000H，（SI）=2345H，内存单元12445H的内容为2715H，问该指令执行后，BX的值是什么?



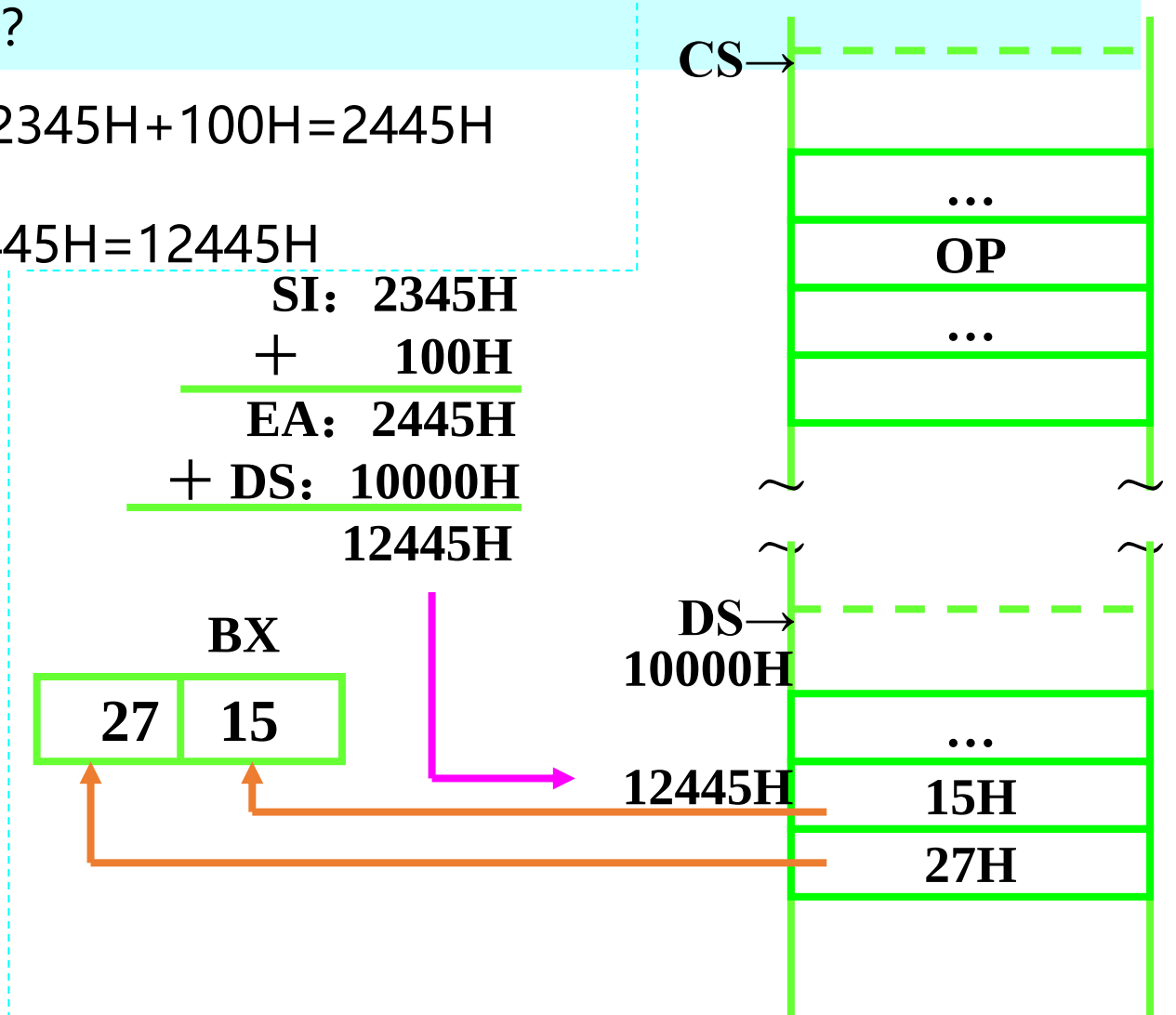
与数据有关的寻址方式

【例3.5】假设指令：MOV BX, [SI+100H]，在执行它时，（DS）=1000H，（SI）=2345H，内存单元12445H的内容为2715H，问该指令执行后，BX的值是什么?

解：EA=（SI）+100H=2345H+100H=2445H

PA=（DS）*16+EA=1000H*16+2445H=12445H

所以，该指令的执行效果是：把从物理地址为12445H开始的一个字的值传送给BX。



与数据有关的寻址方式

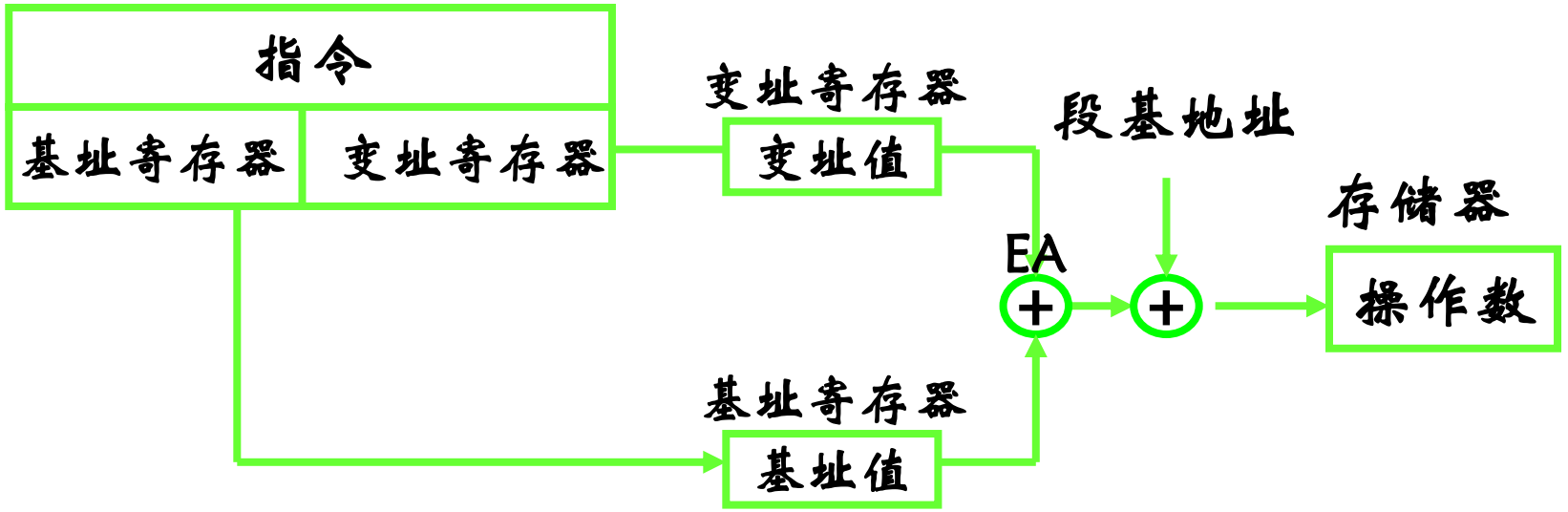
(4) 基址变址寻址方式

定义：操作数在存储器中，其有效地址是一个基址寄存器（BX、BP）和一个变址寄存器（SI、DI）的内容之和。

汇编格式： [BR+IR]

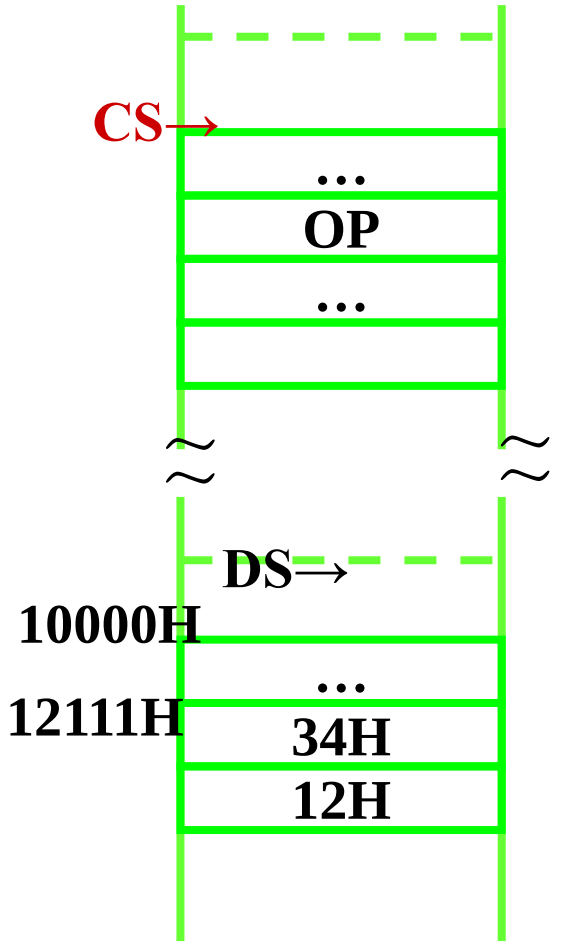
功能：操作数存放在存储器，BR的内容加IR的内容是操作数的偏移地址EA。

图形表示：



与数据有关的寻址方式

【例】假设指令：MOV BX, [BX+SI]，在执行时，（DS）=1000H，（BX）=2100H，（SI）=0011H，内存单元12111H的内容为1234H。问该指令执行后，BX的值是什么?



与数据有关的寻址方式

【例】假设指令：MOV BX, [BX+SI]，在执行时，（DS）=1000H，（BX）=2100H，（SI）=0011H，内存单元12111H的内容为1234H。问该指令执行后，BX的值是什么?

解：操作数的物理地址PA为：

PA=(DS)*16+(BX)+(SI)

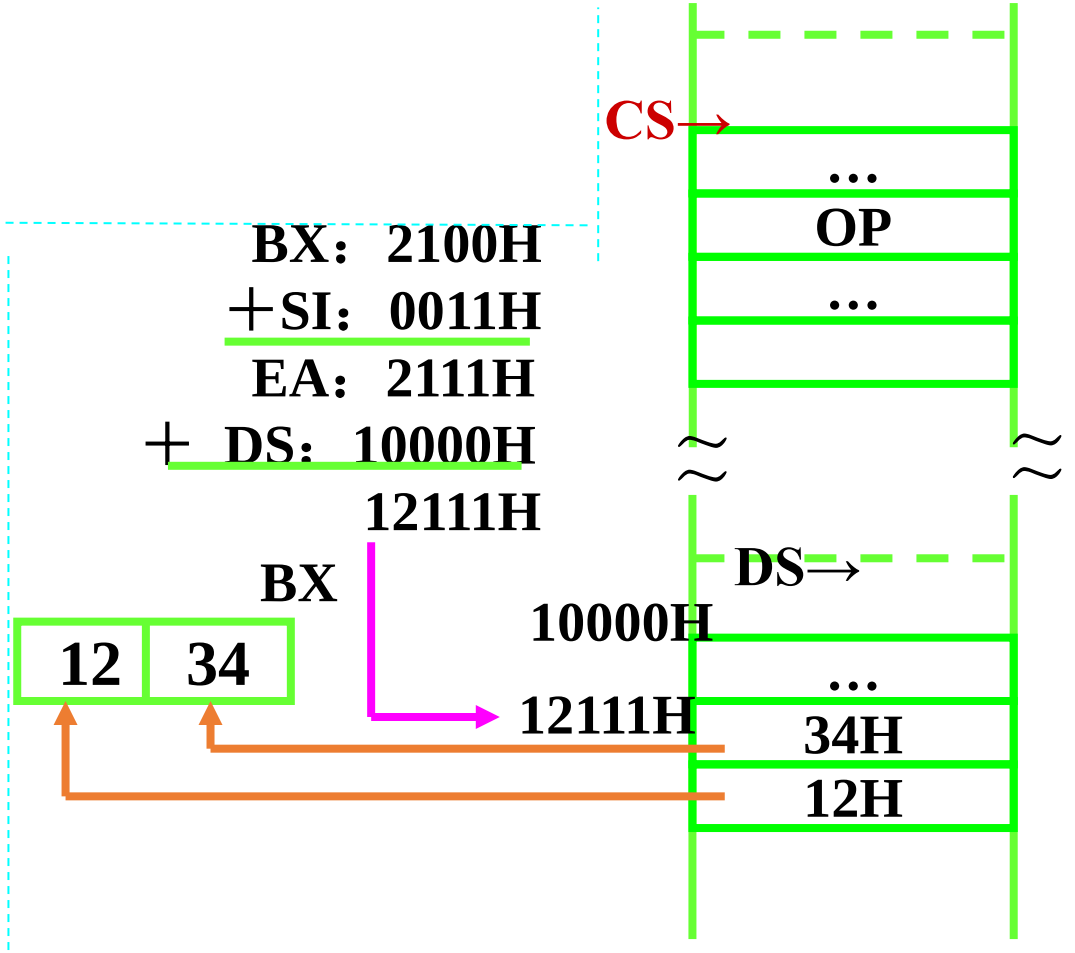
=1000H*16+2100H+0011H

=12111H

所以，该指令的执行效果是：

把从物理地址为12111H开始

的一个字的值传送给BX。



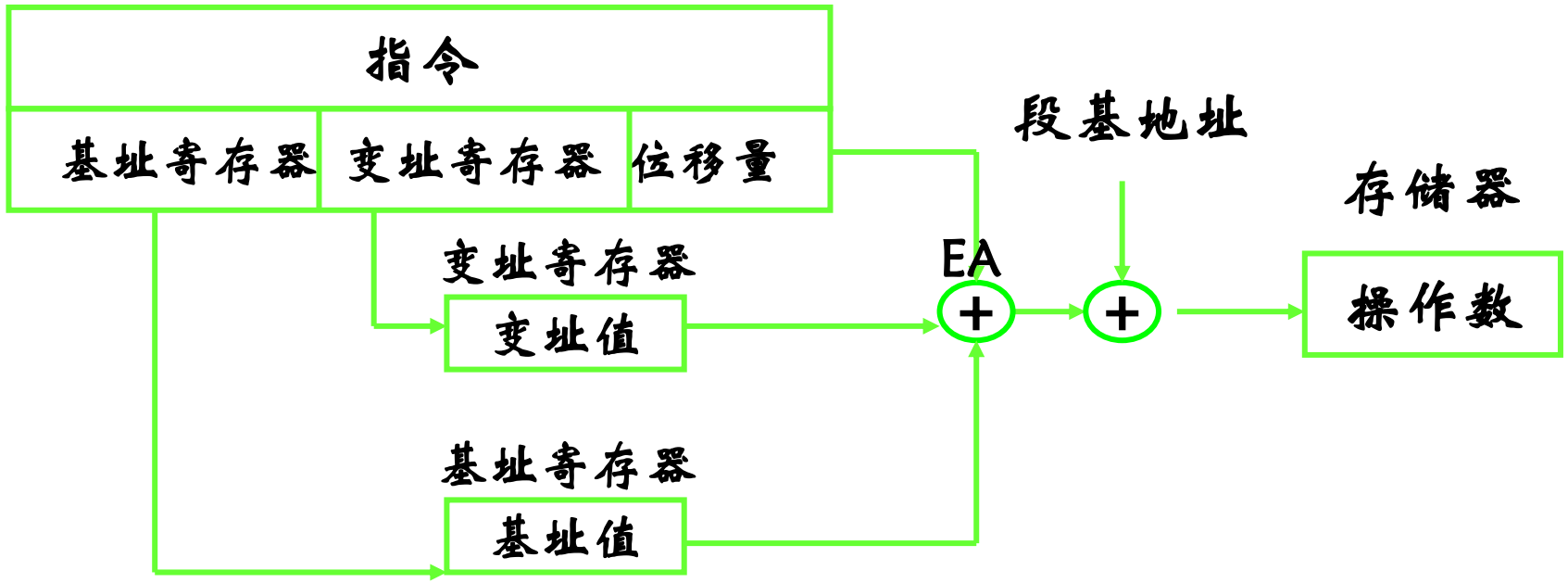
与数据有关的寻址方式

(5) 相对基址变址寻址方式

定义：操作数在存储器中，其有效地址是一个基址寄存器（BX、BP）的值、一个变址寄存器（SI、DI）的值和指令中的8位/16位位移量之和。

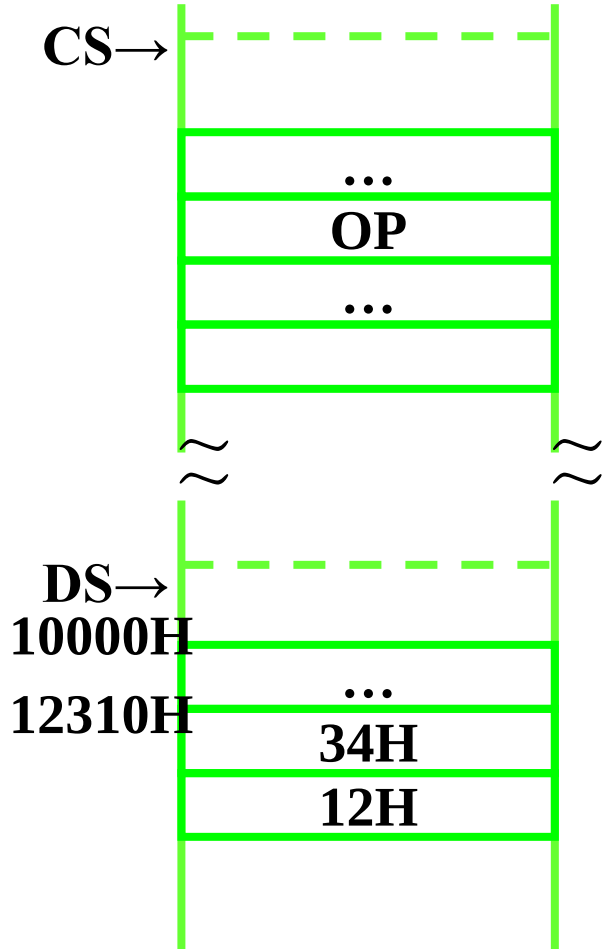
汇编格式：X [BR+IR]或[BR+IR+X]

功能：操作数存放在存储器，BR内容加IR内容加位移量X是操作数的偏移地址EA。



与数据有关的寻址方式

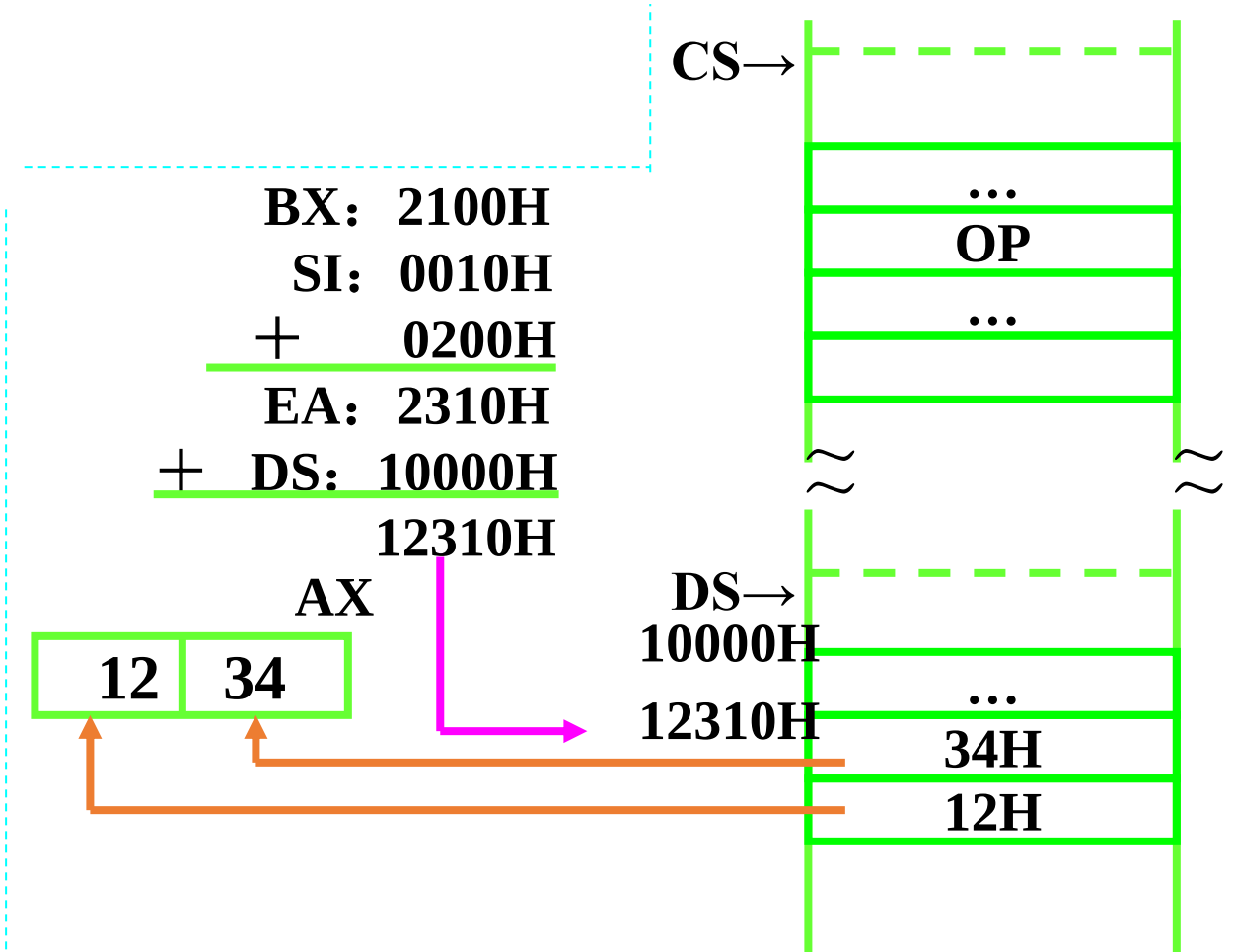
【例3.7】假设指令：MOV AX，[BX+SI+200H]，在执行时，（DS）=1000H，（BX）=2100H，（SI）=0010H，内存单元12310H的内容为1234H。问该指令执行后，AX的值是什么?



与数据有关的寻址方式

【例3.7】假设指令：MOV AX，[BX+SI+200H]，在执行时，（DS）=1000H，（BX）=2100H，（SI）=0010H，内存单元12310H的内容为1234H。问该指令执行后，AX的值是什么?

解：该操作数的物理地址应由DS和EA的值形成，即：
PA=12310H



所以，该指令的执行效果是：把从物理地址为12310H开始的一个字的值传送给AX。

与数据有关的寻址方式

规则总结：

- 若有效地址用SI、DI和BX等之一来指定，则其缺省的段寄存器为DS。寻址方式物理地址的计算方法如下：

$$PA=16\times DS+\begin{cases}(BX)\\(SI)\\(DI)\end{cases}$$

- 若有效地址用BP来指定，则其缺省的段寄存器为SS（即：堆栈段）。物理地址：

$$PA=16\times SS+(BP)$$

与数据有关的寻址方式

例： MOV AL，[buffer]

PA= (DS) ×10H + Offset buffer

默认选择DS寄存器的内容为段地址。

MOV AX，[BP]

PA= (SS) ×10H + (BP)

默认选择SS寄存器的内容为段地址。

与数据有关的寻址方式

❖ 段跨越问题

当要否定默认状态，到非约定段寻找操作数时，必须用跨段前缀指明操作数的段寄存器名。

汇编格式：段寄存器名：操作数地址。

功能：冒号“：”之前的段寄存器名指明操作数所在的段。

【例】 MOV AX，DS:[BP]

MOV CX，SS :[SI]

该例中“DS:”，“SS:”均为跨段前缀，此时默认状态无效，操作数的物理地址PA由段寄存器内容左移4位加偏移EA形成。上述2条指令的源操作数物理地址分别为：

PA1 =（DS）左移4位+(BP)

PA2 =（SS）左移4位+ (SI)

与数据有关的寻址方式

在某些情况下，8086/8088允许程序员使用跨越段前缀来改变系统指定的默认段。但以下3种情况不允许使用跨越段前缀。

①指令必须在代码段CS中；

②PUSH指令的源操作数和POP指令的目的操作数必须使用SS段；

③串处理指令的目的串必须使用附加段ES。

访存类型	所用段及寄存器	缺省选择规则
指令	代码段：CS	用于取指令
堆栈	堆栈段：SS	进栈或出栈，用SP、BP作为基址寄存器的访存
局部数据	数据段：DS	除堆栈或串处理操作以外的所有数据访问
目的串	附加段：ES	串处理指令的目的串

与数据有关的寻址方式

▲综上，按给出偏移地址方式的不同，分为以下5种：

直接寻址	MOV AL, [buffer]
寄存器间接寻址	MOV AL, [BX]
寄存器相对寻址	MOV AL, [BX + 10H]
基址变址寻址	MOV AL, [BX + SI]
相对基址变址寻址	MOV AL, [BX + SI + 10H]

其中：

寄存器相对寻址、基址变址寻址可用于表格或数组。

相对基址变址可用于二维数组。

与数据有关的寻址方式

注意：1）不能自创寻址方式

寄存器操作数地址只能由BX、BP、SI、DI 给出，它们的组合也不是任意的。

寄存器间接
- [SI]
- [DI]
- [BX]
- [BP]

寄存器相对
- [SI + X]
- [DI + X]
- [BX + X]
- [BP + X]

基址加变址
- [BX+SI]
- [BX+DI]
- [BP+SI]
- [BP+DI]

相对基址加变址
- [BX+SI+X]
- [BX+DI+X]
- [BP+SI+X]
- [BP+DI+X]

其中X为8位或16位偏移量

与数据有关的寻址方式

2）只有存储器操作数需用段跨越的前缀

哪些正确？哪些错误？

MOV ES:[SI], CX

MOV AL, DS:[BP]

MOV ES:AX, 0

MOV Ds:CX, 22H

与数据有关的寻址方式

2）只有存储器操作数需用段跨越的前缀

MOV ES:[SI], CX √

MOV AL, DS:[BP] √

MOV ES:AX, 0 ×

MOV Ds:CX, 22H ×

与数据有关的寻址方式

3)哪些正确？哪些错误?

如　MOV　CL, [AX]

MOV　AX, [DX]

MOV　AL, [CX]

MOV　CX, [BP+BX]

MOV　AH, [SI+DI]

MOV　BL, [AX+CX]

与数据有关的寻址方式

3)常见错误：

如　MOV　CL，[AX]

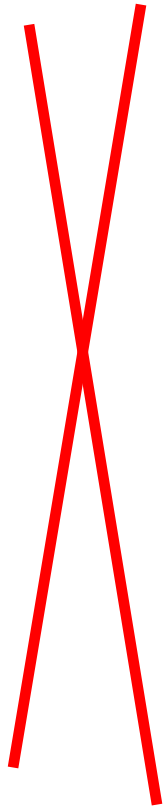
MOV　AX，[DX]

MOV　AL，[CX]

MOV　CX，[BP+BX]

MOV　AH，[SI+DI]

MOV　 BL，[AX+CX]



Q&A