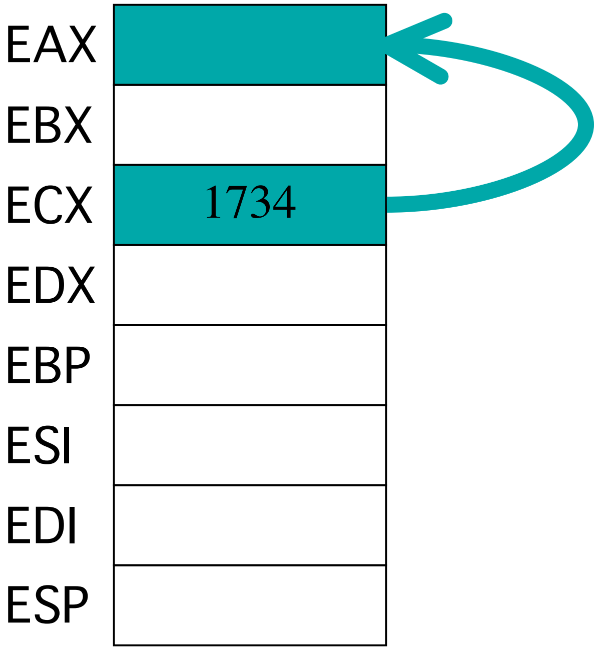
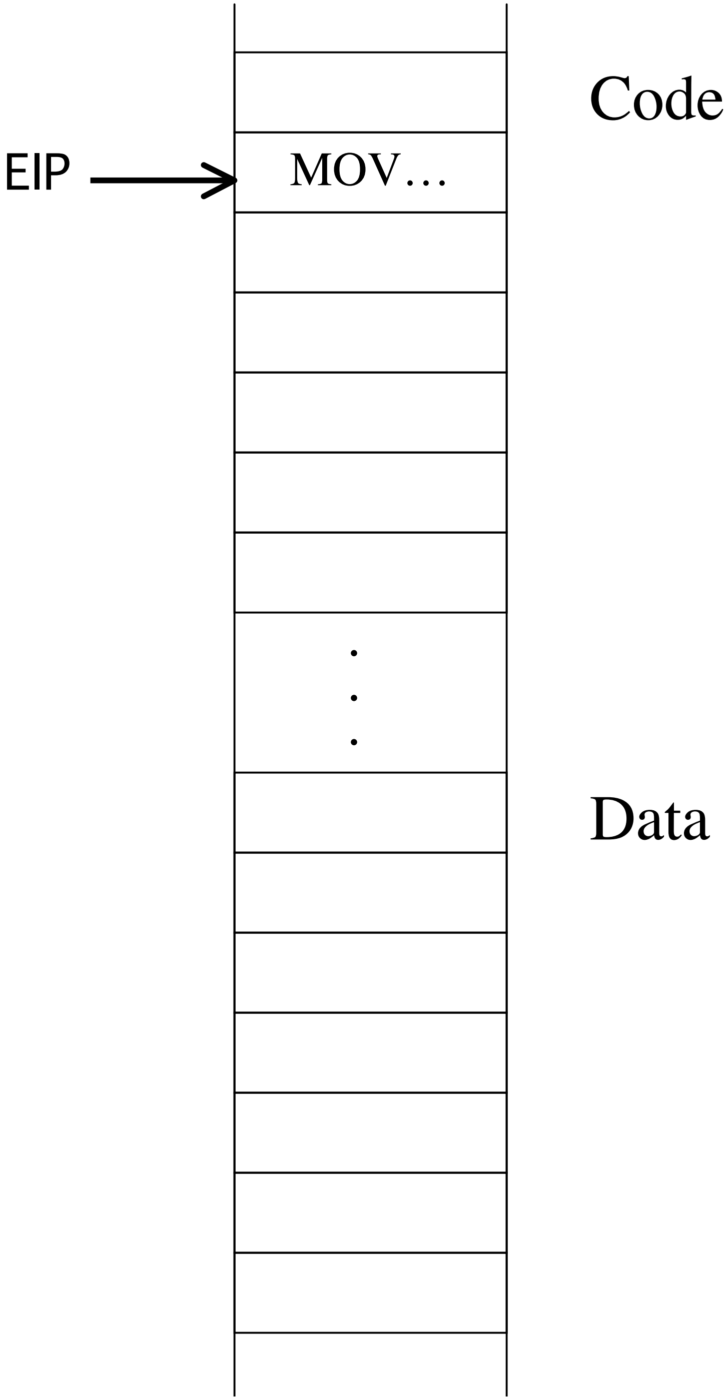
Addressing Modes

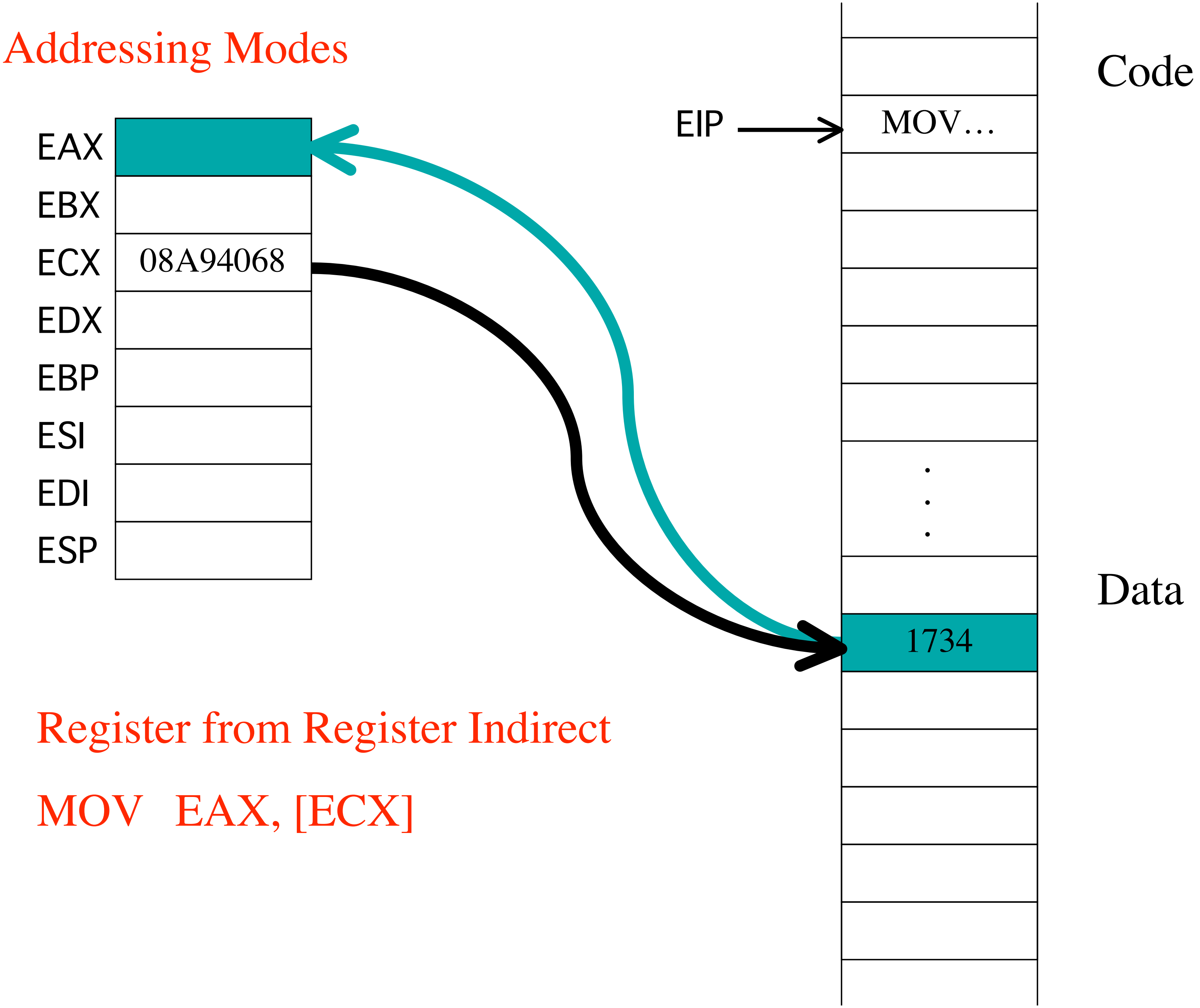




Register from Register

MOV EAX, ECX

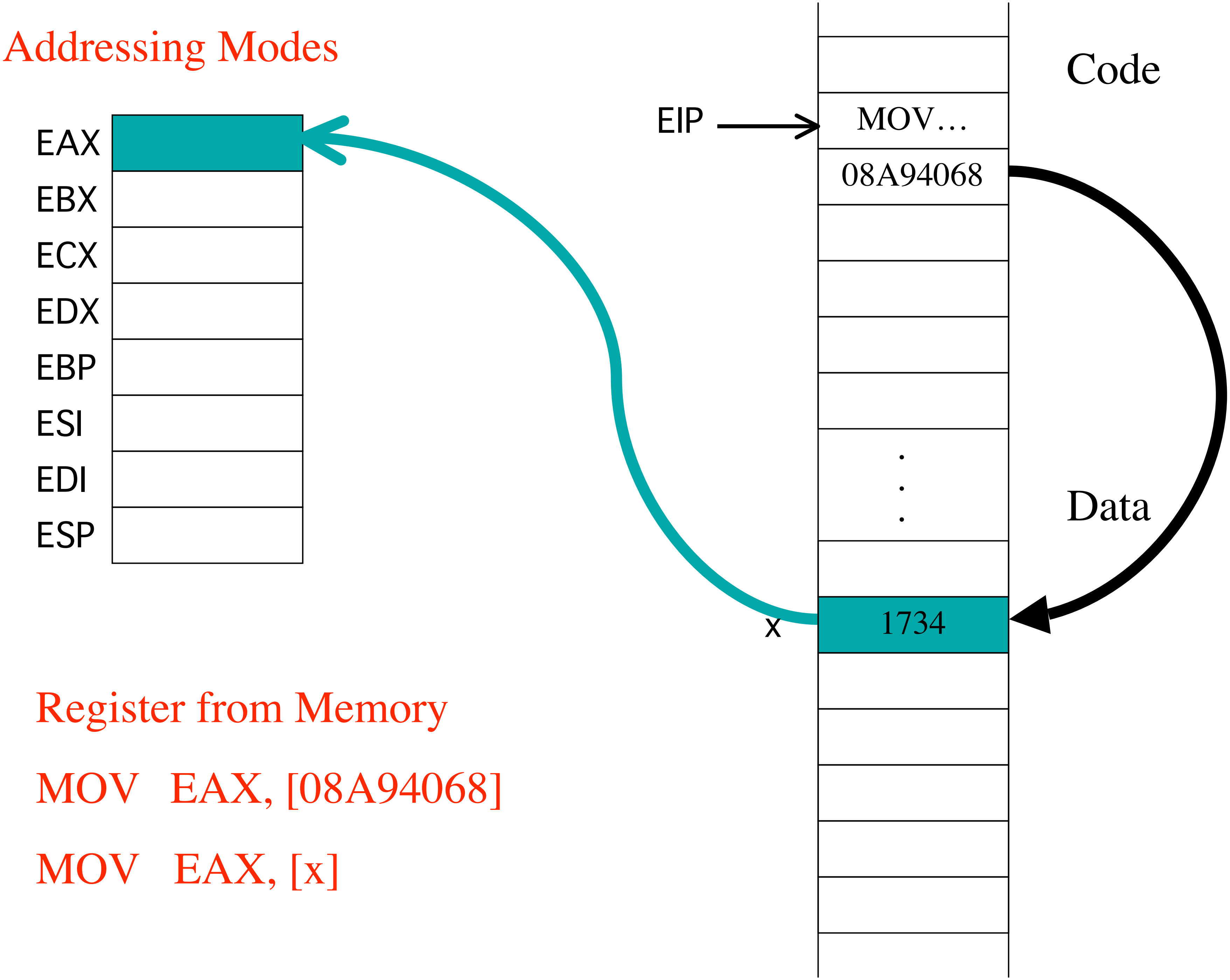
Addressing Modes



Register from Register Indirect

MOV EAX, [ECX]

Addressing Modes

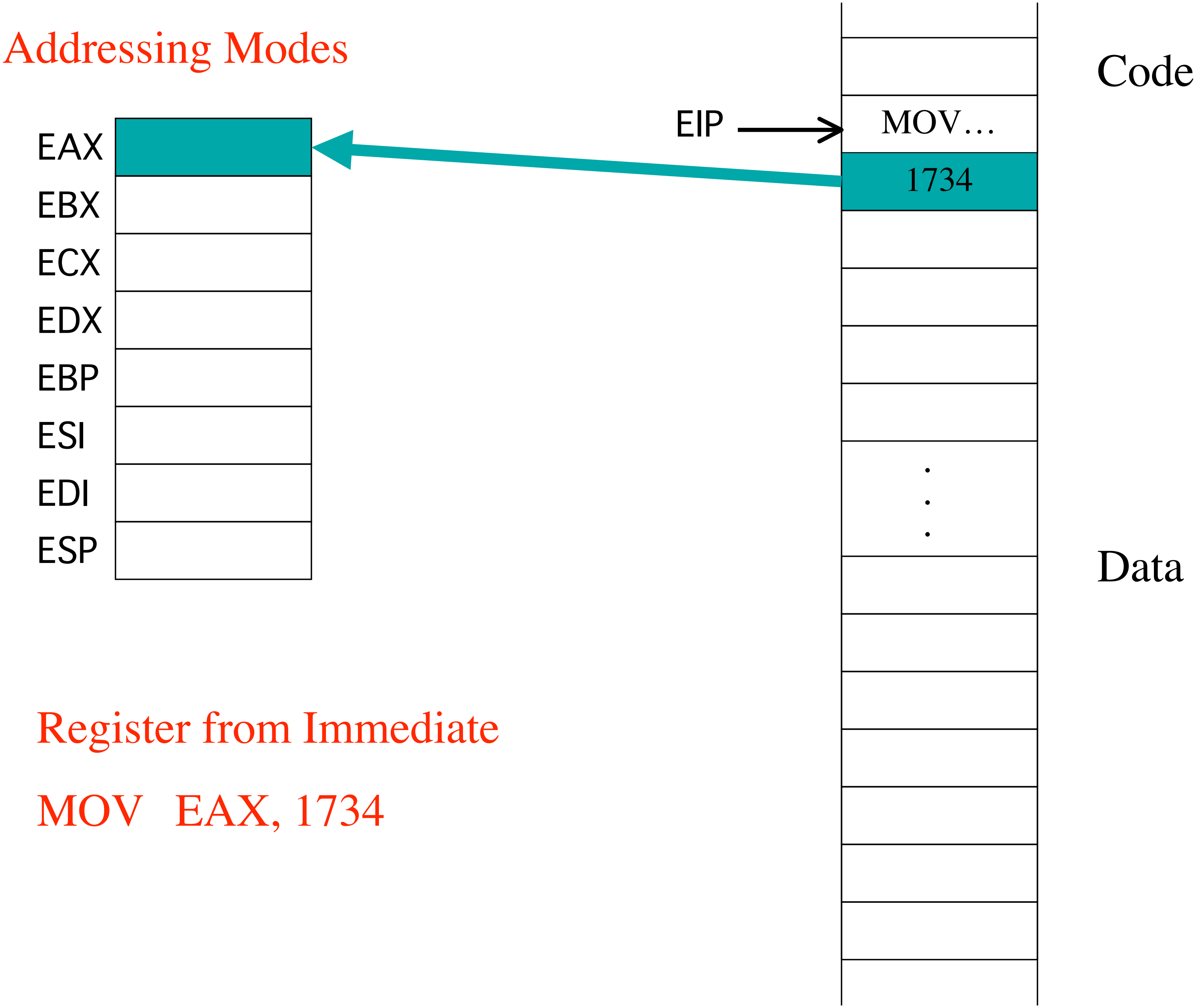


Register from Memory

MOV   EAX, [08A94068]

MOV   EAX, [x]

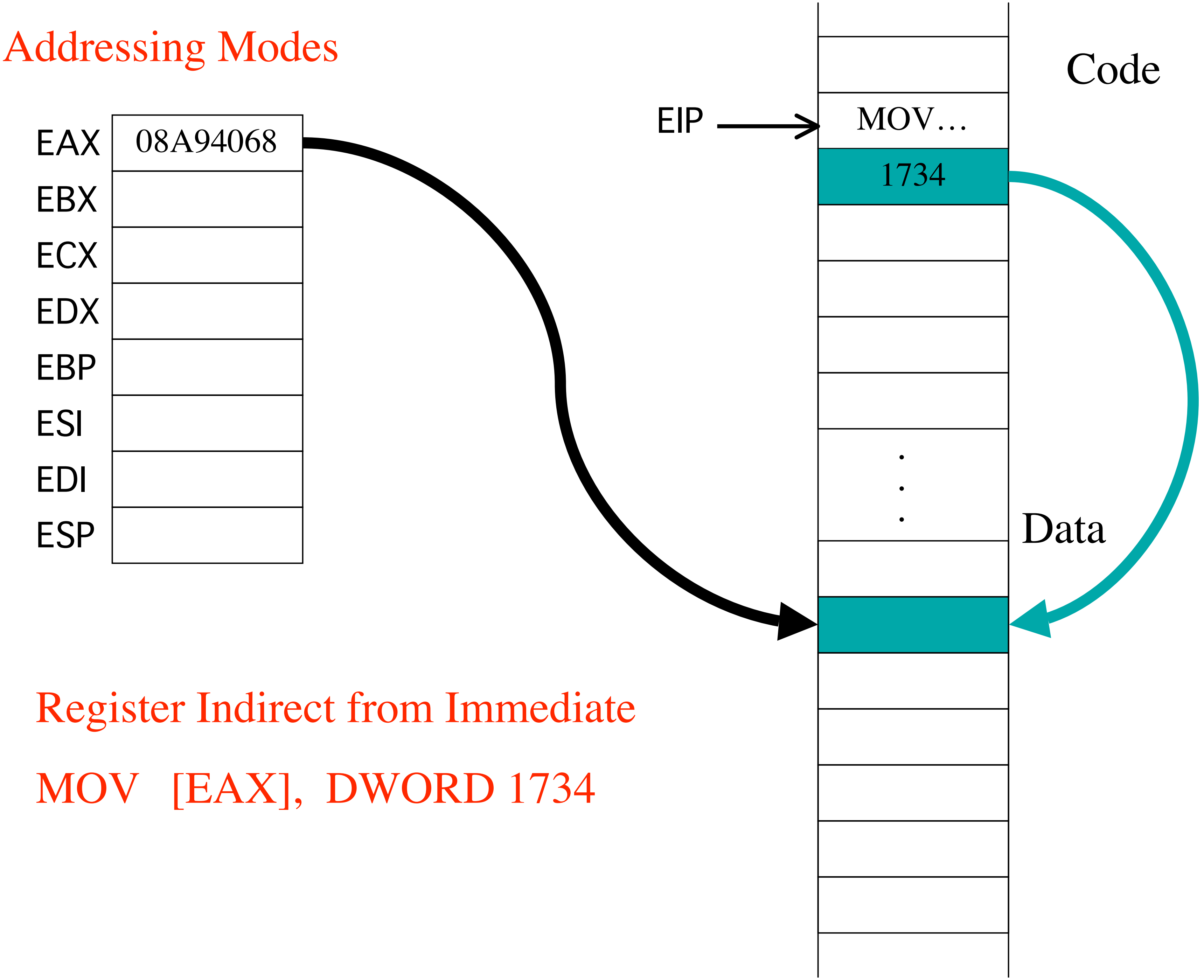
Addressing Modes



Register from Immediate

MOV EAX, 1734

Addressing Modes



EAX	08A94068
EBX	
ECX	
EDX	
EBP	
ESI	
EDI	
ESP	

EIP

MOV…

1734

Code

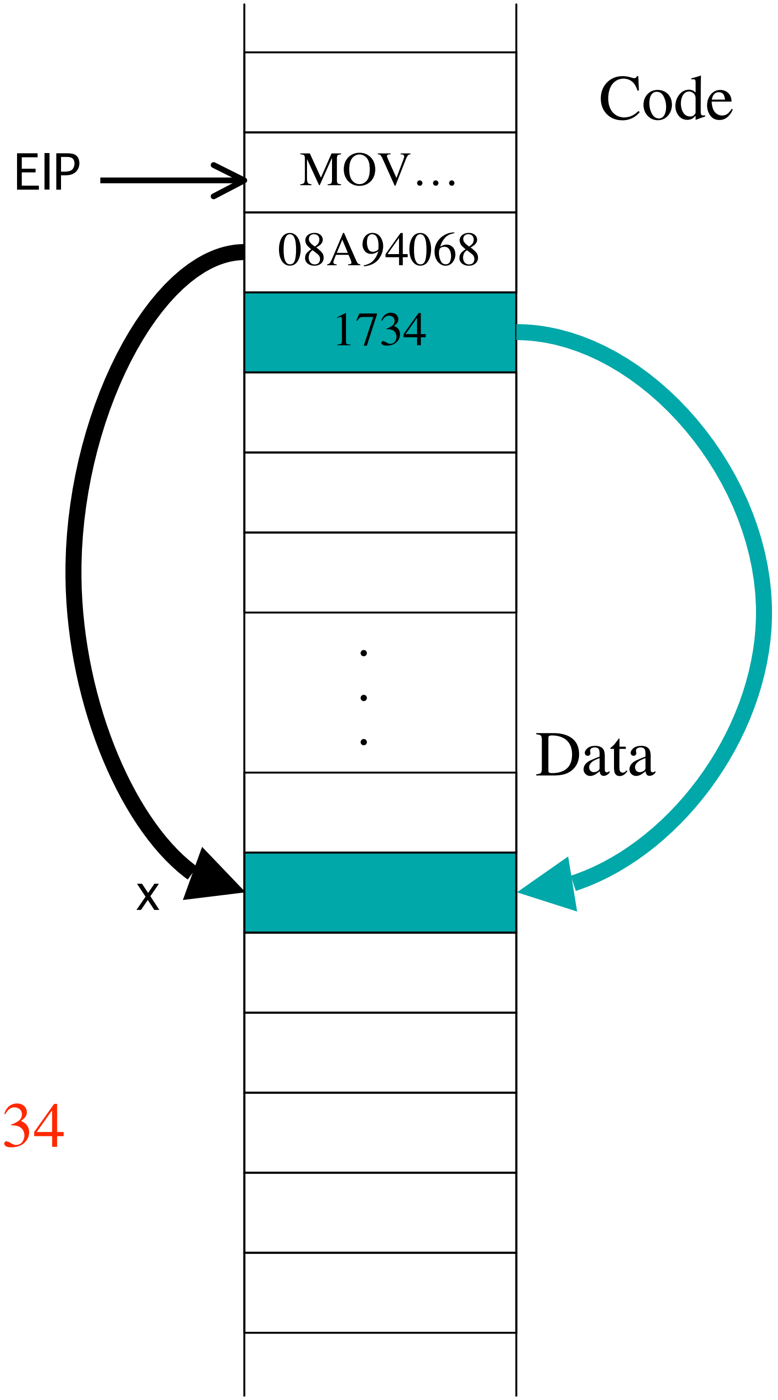
Data

Register Indirect from Immediate

MOV [EAX], DWORD 1734

Addressing Modes

EAX	
EBX	
ECX	
EDX	
EBP	
ESI	
EDI	
ESP	



Register Indirect from Immediate

MOV [08A94068], DWORD 1734

MOV [x], DWORD 1734

Indexed Addressing

- Operands of the form: [ESI + ECX*4 + DISP]
- ESI = Base Register
- ECX = Index Register
- 4 = Scale factor
- DISP = Displacement
- The operand is in memory
- The address of the memory location is
  ESI + ECX*4 + DISP

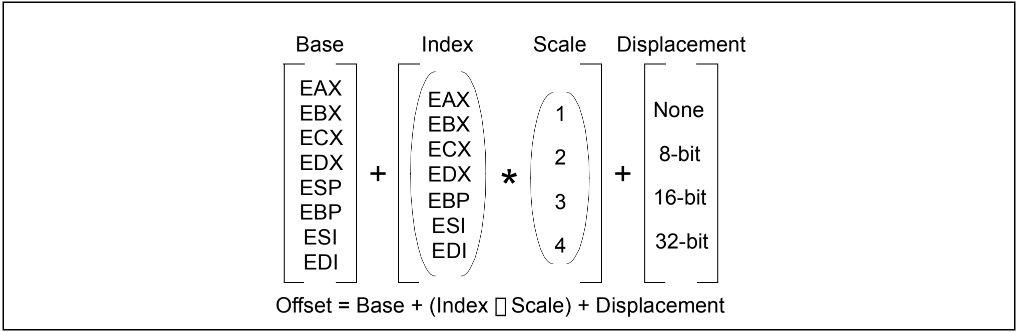


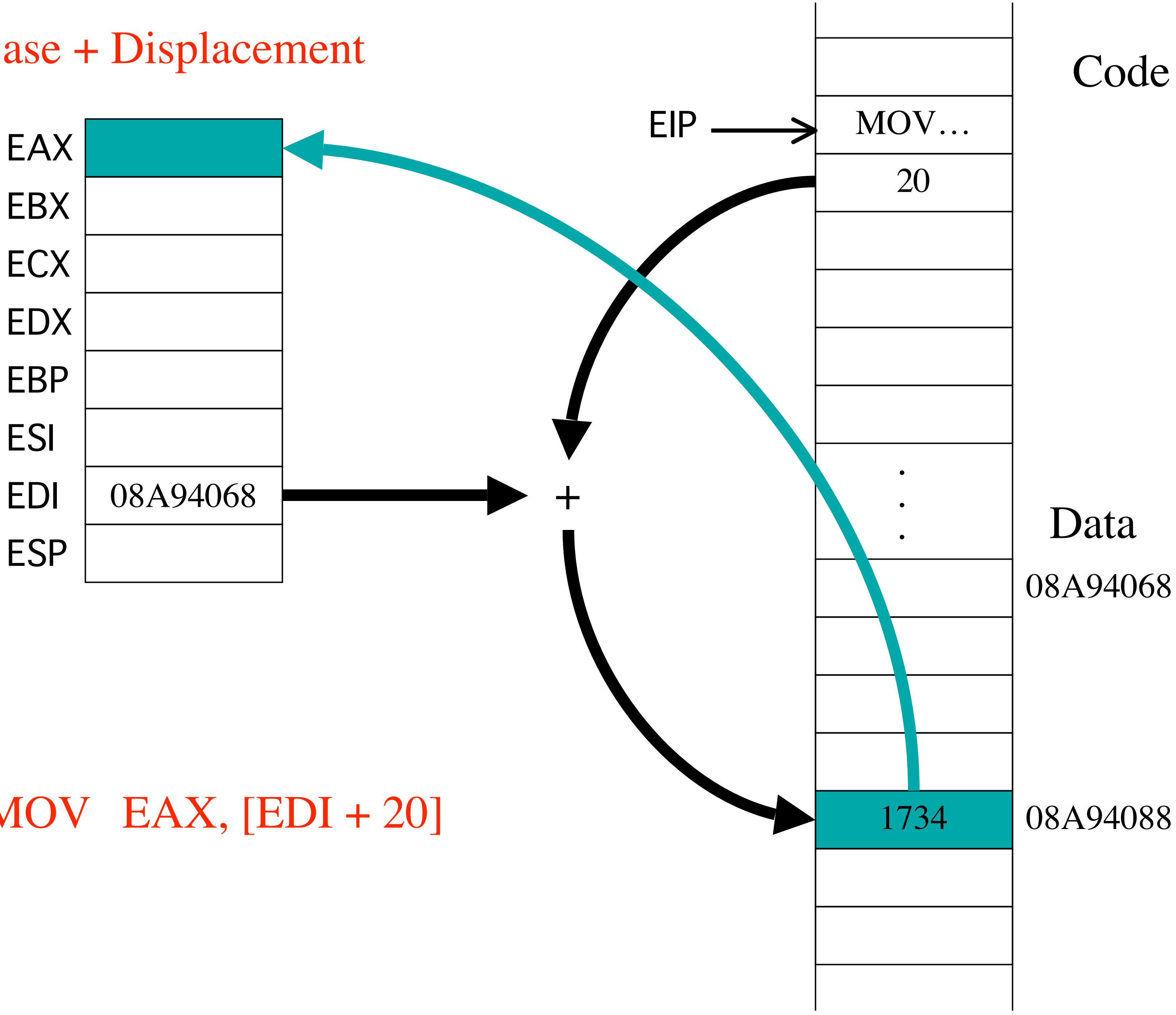
Figure 3-9. Offset (or Effective Address) Computation

The uses of general-purpose registers as base or index components are restricted in the following manner:

- The ESP register cannot be used as an index register.
- When the ESP or EBP register is used as the base, the SS segment is the default segment. In all other cases, the DS segment is the default segment.

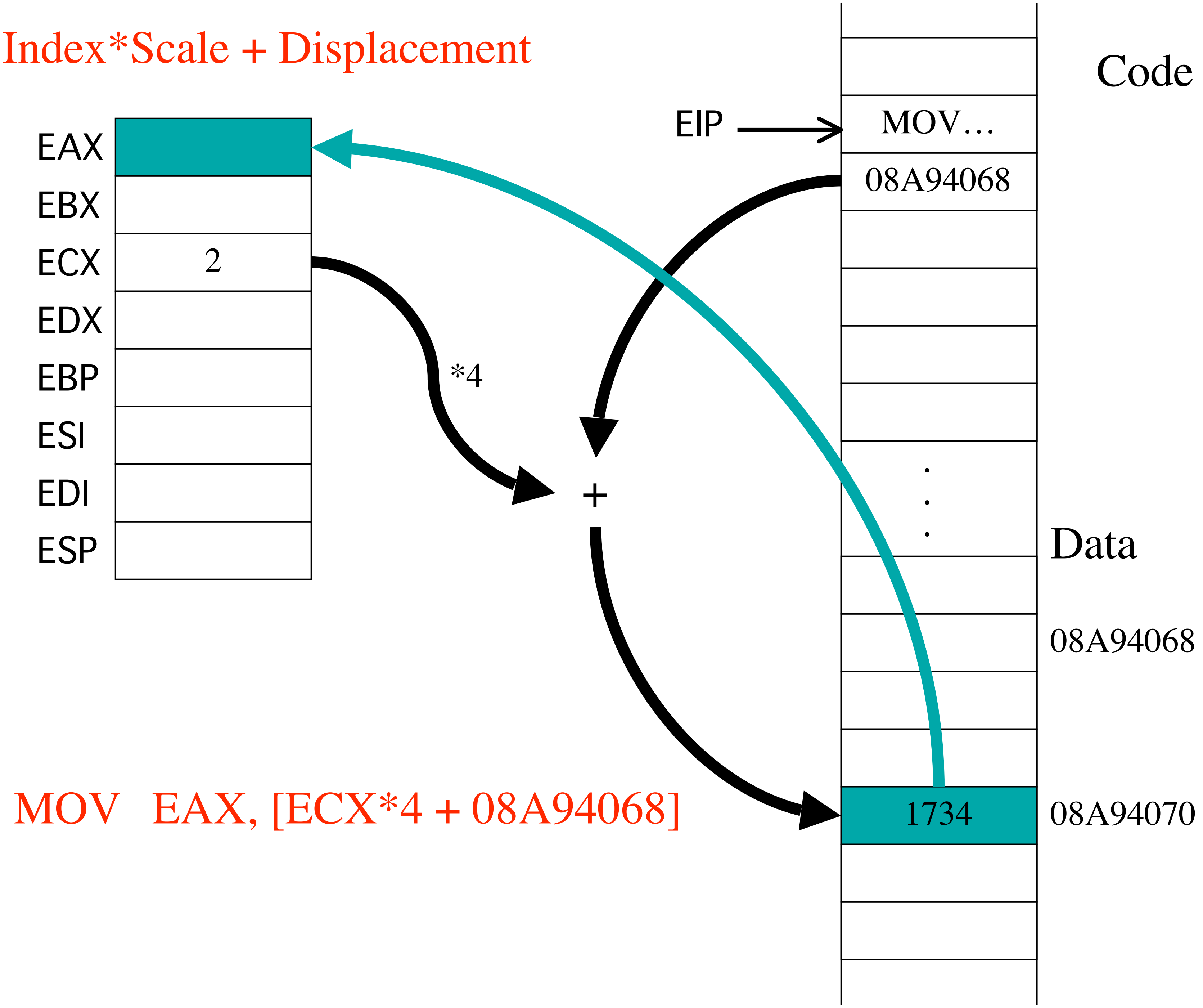
The base, index, and displacement components can be used in any combination, and any of these components can be null. A scale factor may be used only when an index also is used. Each possible combination is useful for data structures commonly used by programmers in high-level languages and assembly language. The following addressing modes suggest uses for common combinations of address components.

Base + Displacement



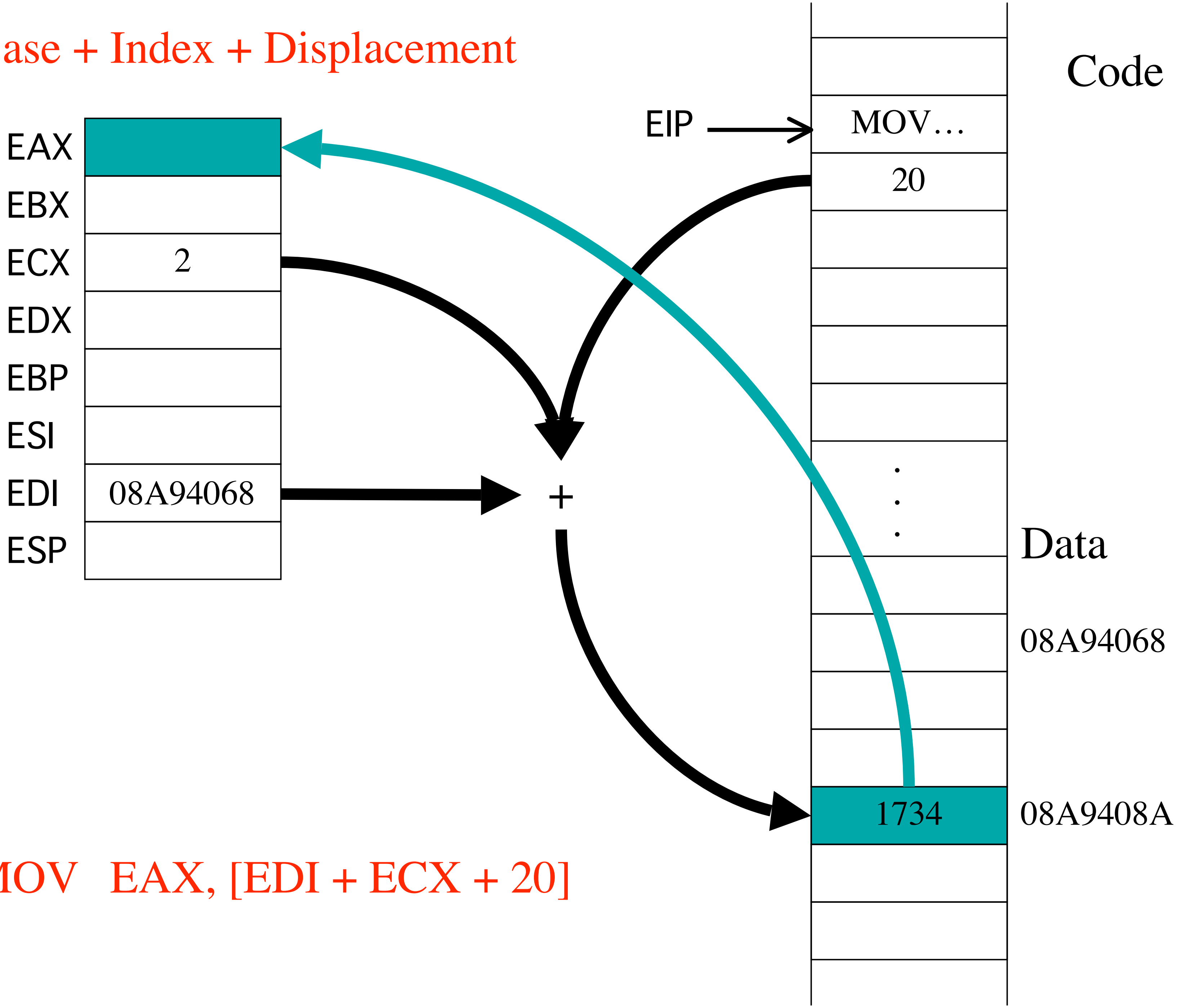
MOV   EAX, [EDI + 20]

Index*Scale + Displacement



MOV   EAX, [ECX*4 + 08A94068]

Base + Index + Displacement



EAX	
EBX	
ECX	2
EDX	
EBP	
ESI	
EDI	08A94068
ESP	

+

EIP → MOV…

20

Code

. . .

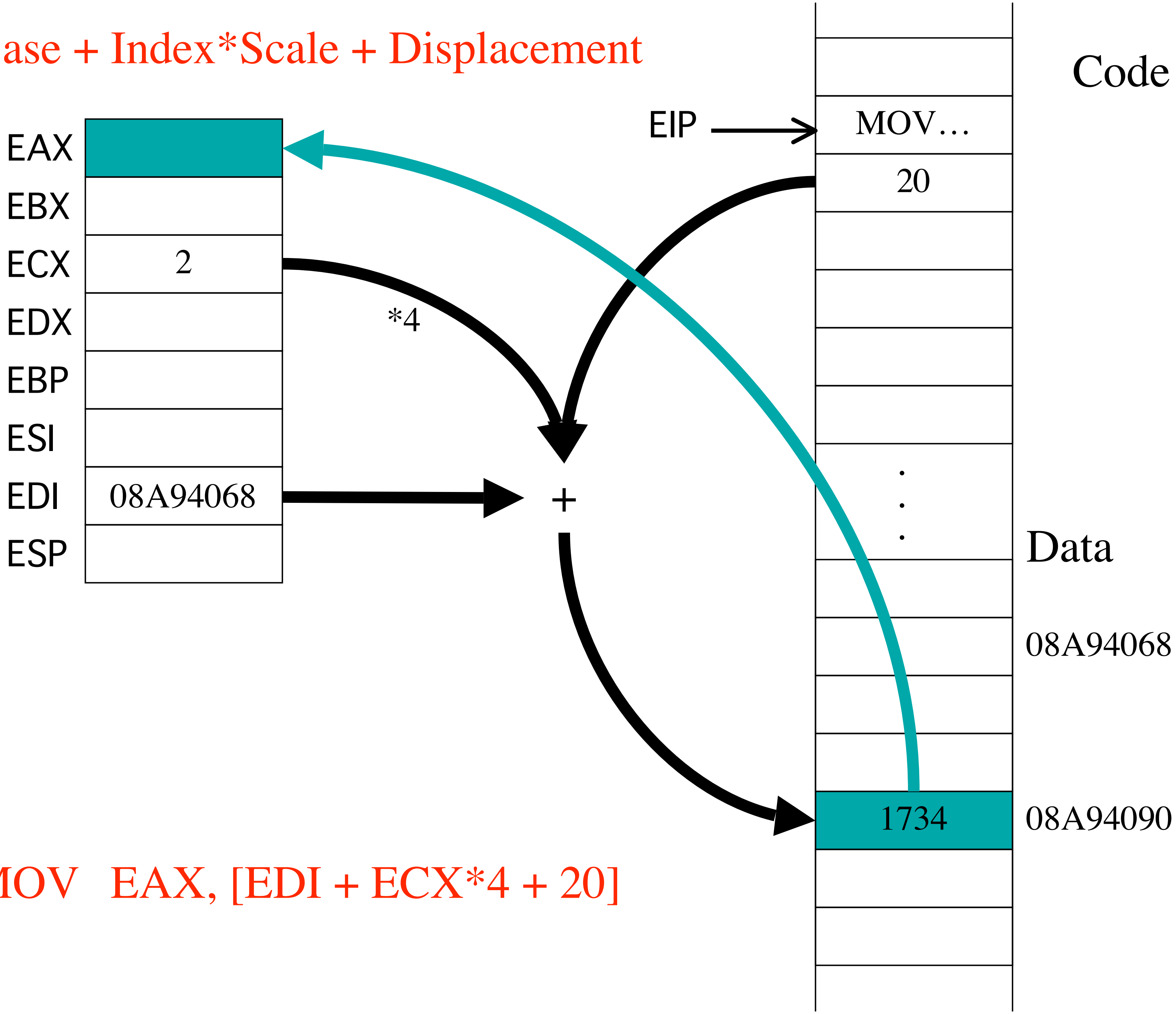
Data

08A94068

1734 08A9408A

MOV EAX, [EDI + ECX + 20]

Base + Index*Scale + Displacement



MOV   EAX, [EDI + ECX*4 + 20]

Typical Uses for Indexed Addressing

- **Base + Displacement**
  - ◇ access character in a string or field of a record
  - ◇ access a local variable in function call stack
- **Index*Scale + Displacement**
  - ◇ access items in an array where size of item is 2, 4 or 8 bytes
- **Base + Index + Displacement**
  - ◇ access two dimensional array (displacement has address of array)
  - ◇ access an array of records (displacement has offset of field in a record)
- **Base + (Index*Scale) + Displacement**
  - ◇ access two dimensional array where size of item is 2, 4 or 8 bytes