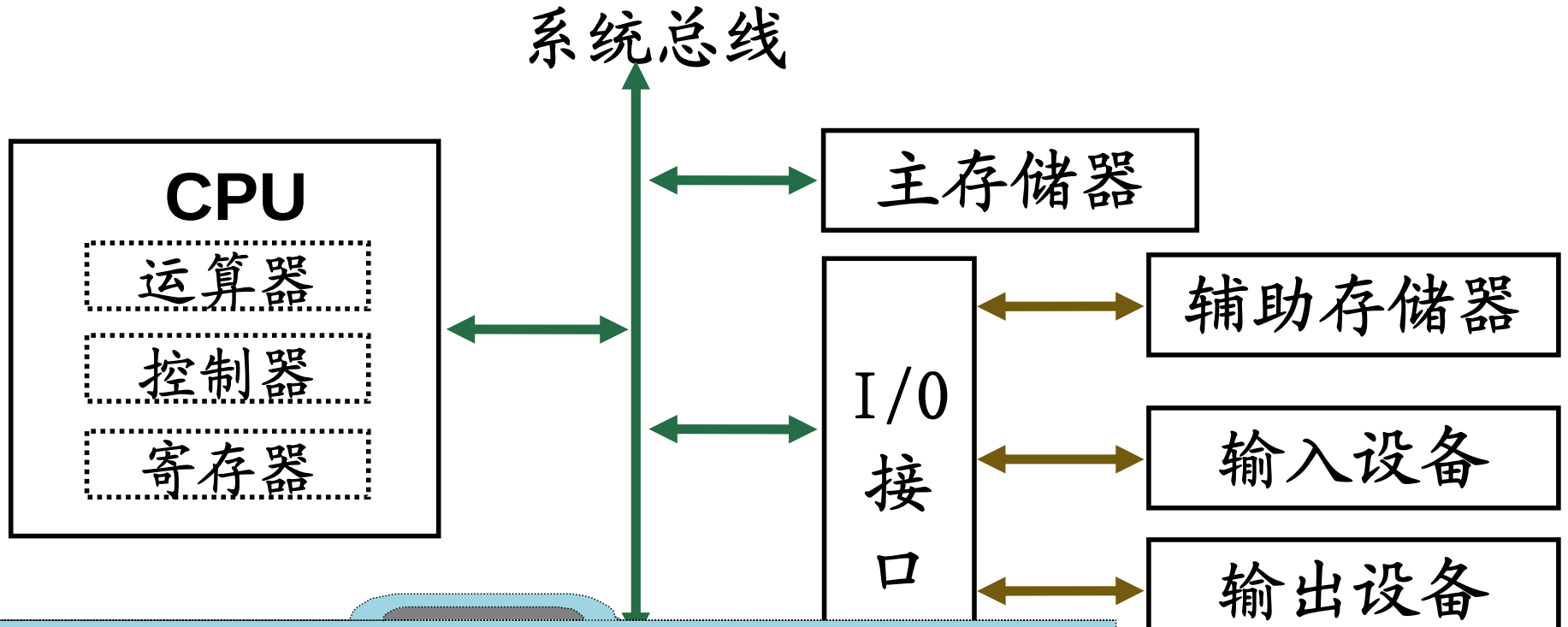
处理器通用寄存器

计算机的硬件组成结构



汇编语言程序员将硬件抽象为：

寄存器、存储器地址和输入输出地址

寄存器（Register）

- 处理器内部的高速存储单元
- 用于暂时存放程序执行过程中的代码和数据
- 透明寄存器
  - 对应用人员不可见、不能编程直接控制
- 可编程（Programmable）寄存器
  - 具有引用名称、供编程使用
    - 通用寄存器（General-Purpose Register）
    - 专用寄存器

IA-32处理器的常用寄存器

寄存器 { 透明寄存器
可编程寄存器 { 通用寄存器
专用寄存器

通用寄存器	32位通用寄存器	EAX EBX ECX EDX ESI EDI EBP ESP
	16位通用寄存器	AX BX CX DX SI DI BP SP
	8位通用寄存器	AH AL BH BL CH CL DH DL
专用寄存器	标志寄存器	EFLAGS
	指令指针寄存器	EIP
	段寄存器	CS DS SS ES FS GS

通用寄存器

- 处理器最常使用的整数通用寄存器
- 可用于保存整数数据、地址等
- 32位IA-32处理器具有8个32位通用寄存器

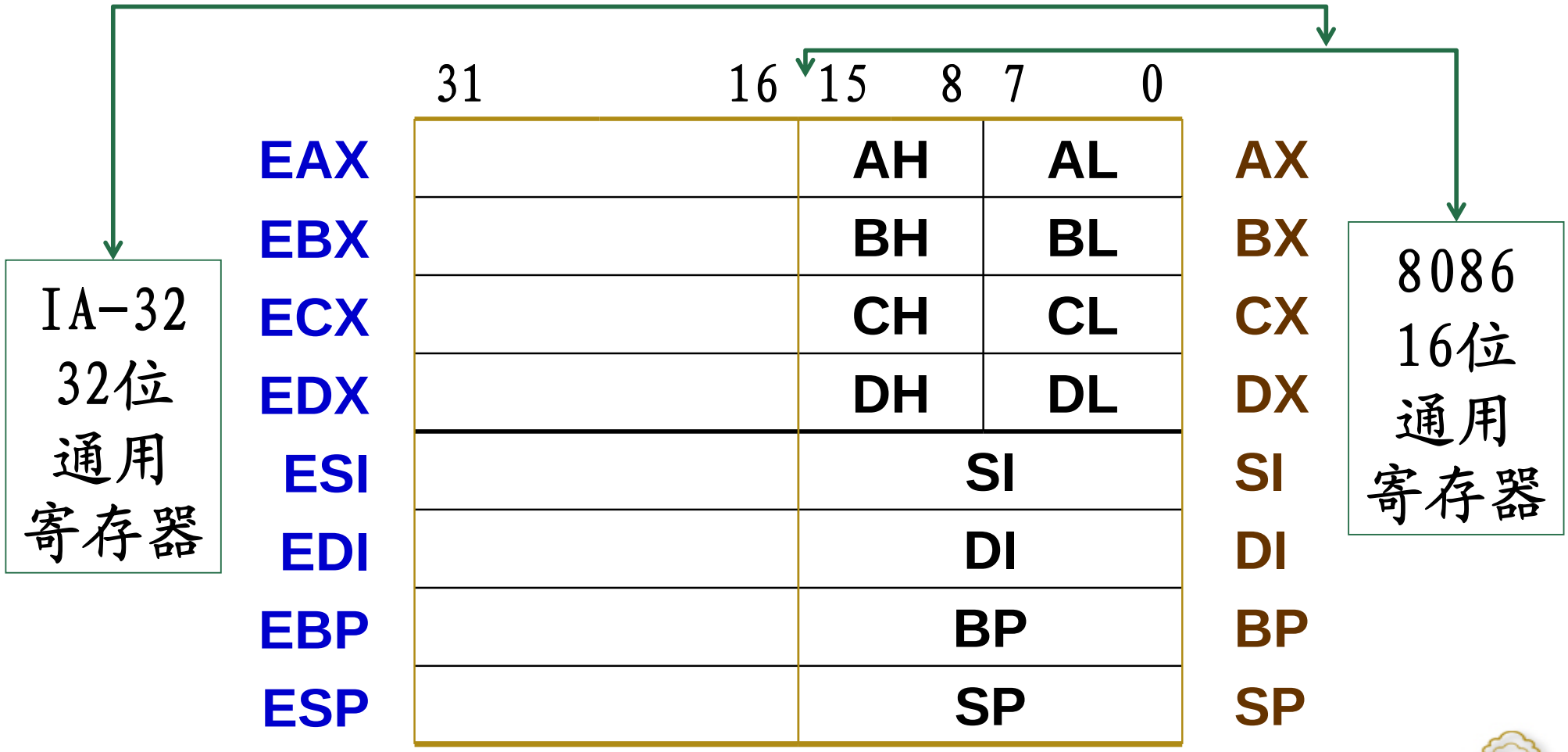
  EAX，EBX，ECX，EDX，ESI，EDI，EBP，ESP
- 它们源自16位8086处理器的8个16位通用寄存器

  AX，BX，CX，DX，SI，DI，BP，SP
- 前4个寄存器还可分成高低字节，形成8个8位通用寄存器

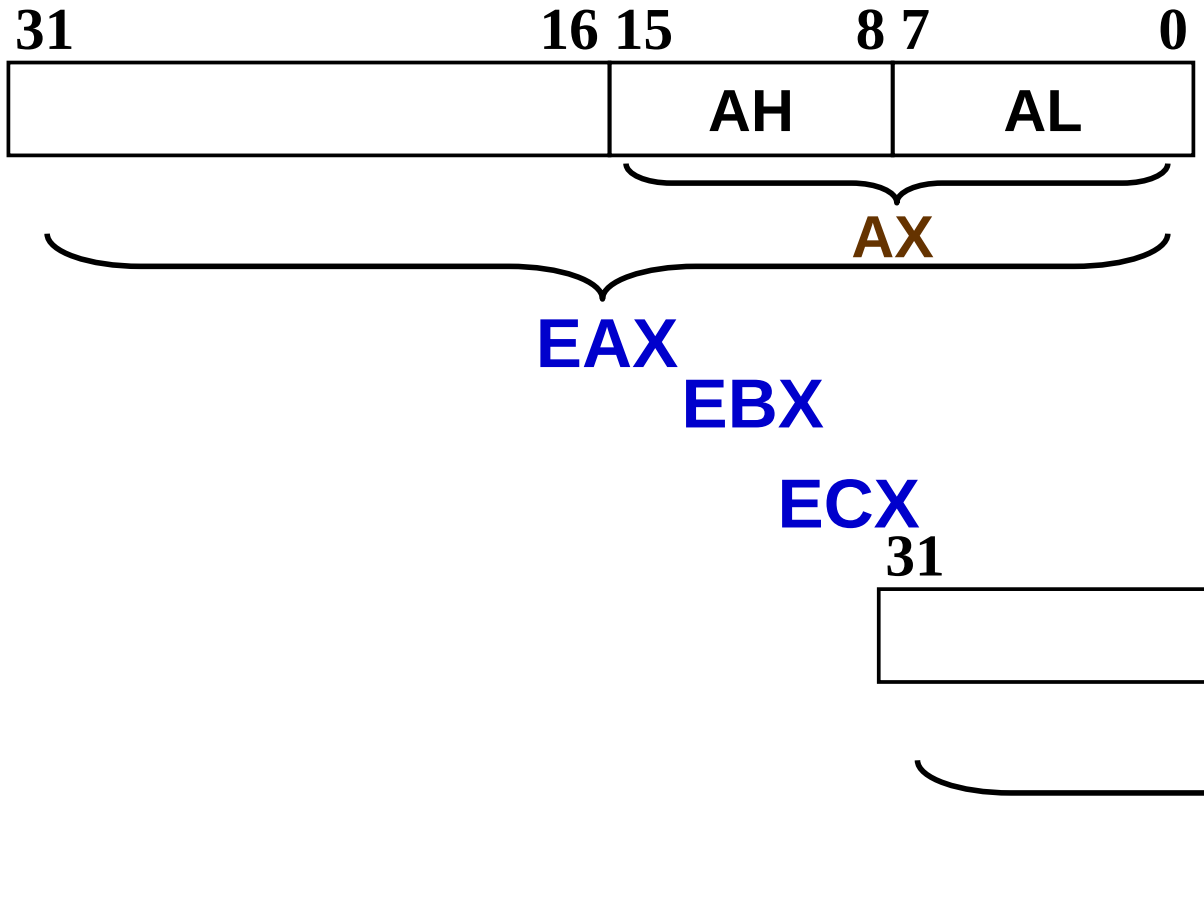
  AH，AL，BH，BL，CH，CL，DH，DL

既是一个整体
又可独立使用

16位扩展（Extended）为32位



前4个分成高（High）低（Low）字节



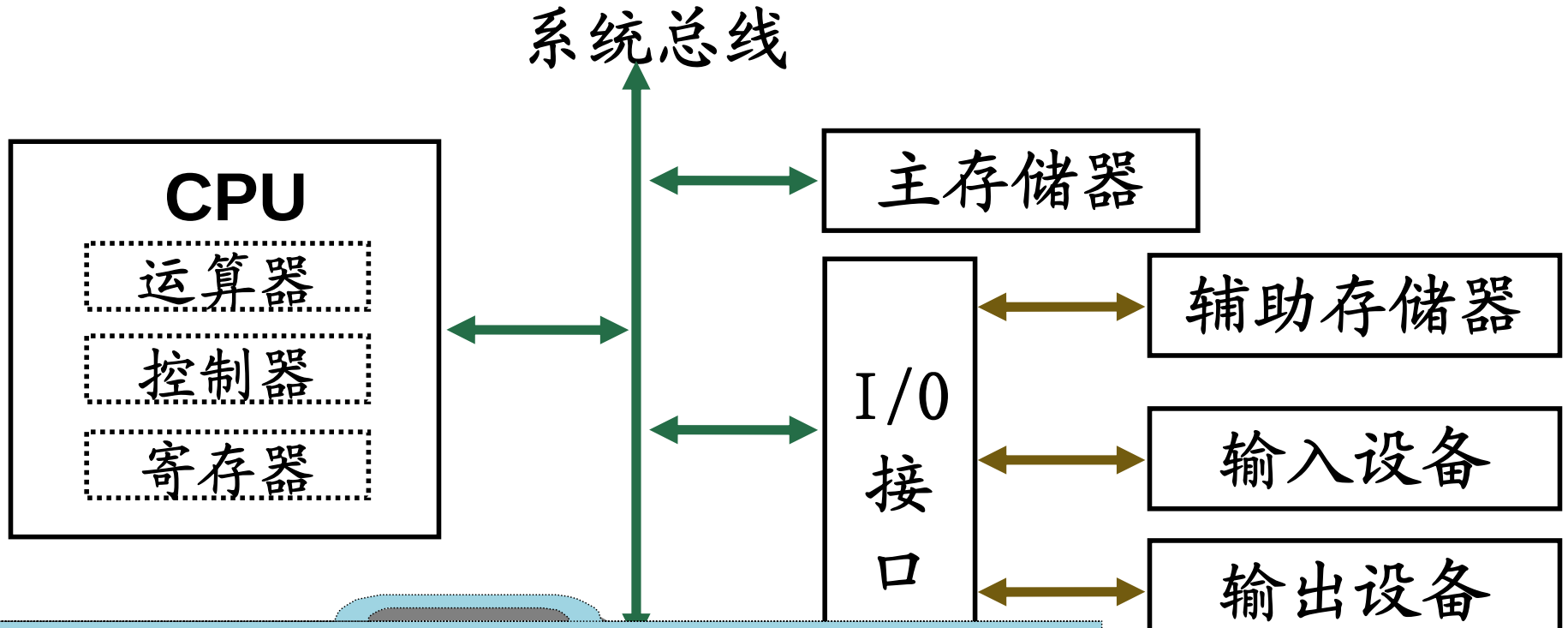
既是一个整体
又可独立使用

通用寄存器的名称

EAX	Accumulator	累加器
EBX	Base Address	基址寄存器
ECX	Counter	计数器
EDX	Data	数据寄存器
ESI	Source Index	源变址寄存器
EDI	Destination Index	目的变址寄存器
EBP	Base Pointer	基址指针
ESP	Stack Pointer	堆栈指针

存储器组织

计算机的硬件组成结构



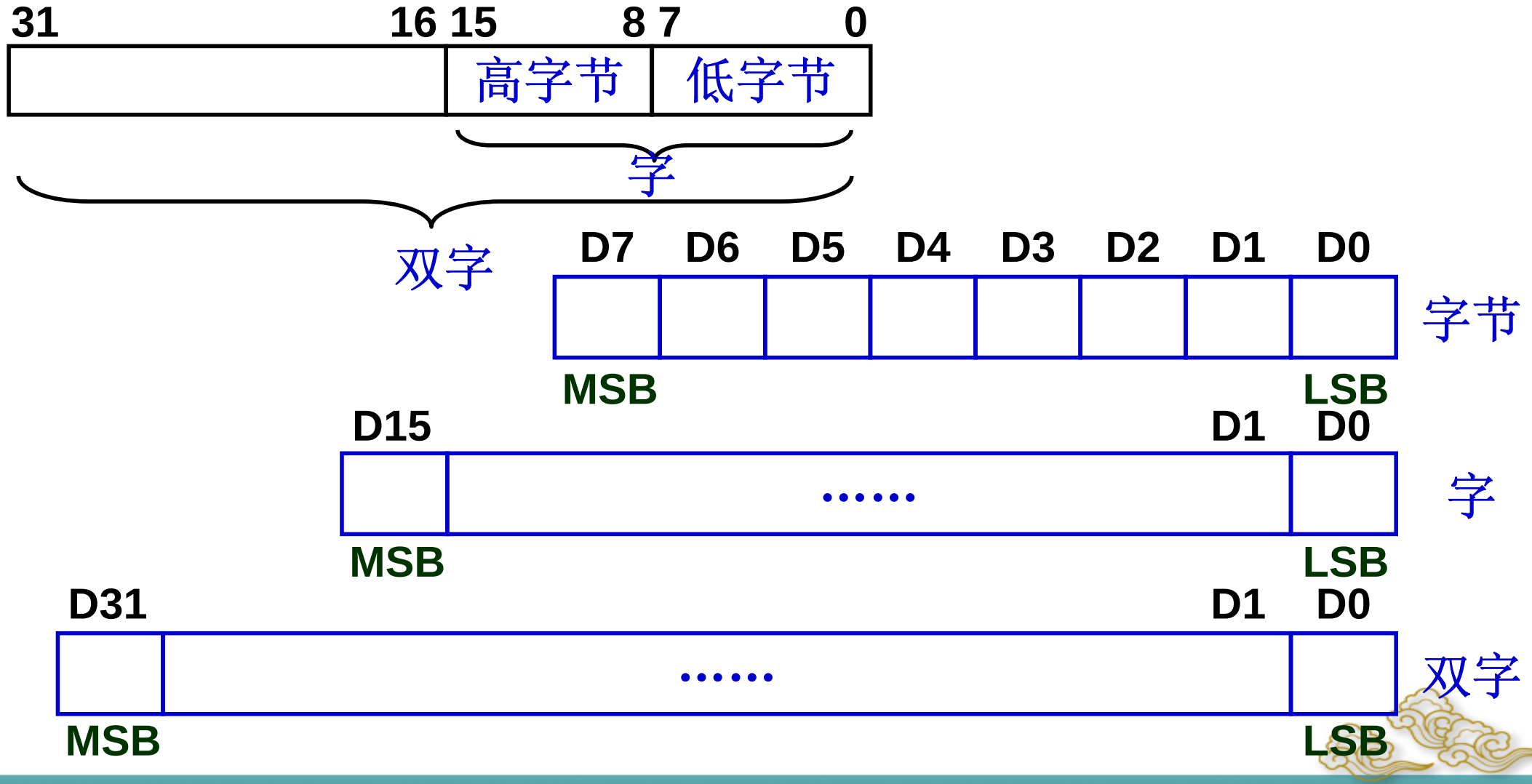
汇编语言程序员将硬件抽象为：

寄存器、存储器地址和输入输出地址

存储器地址

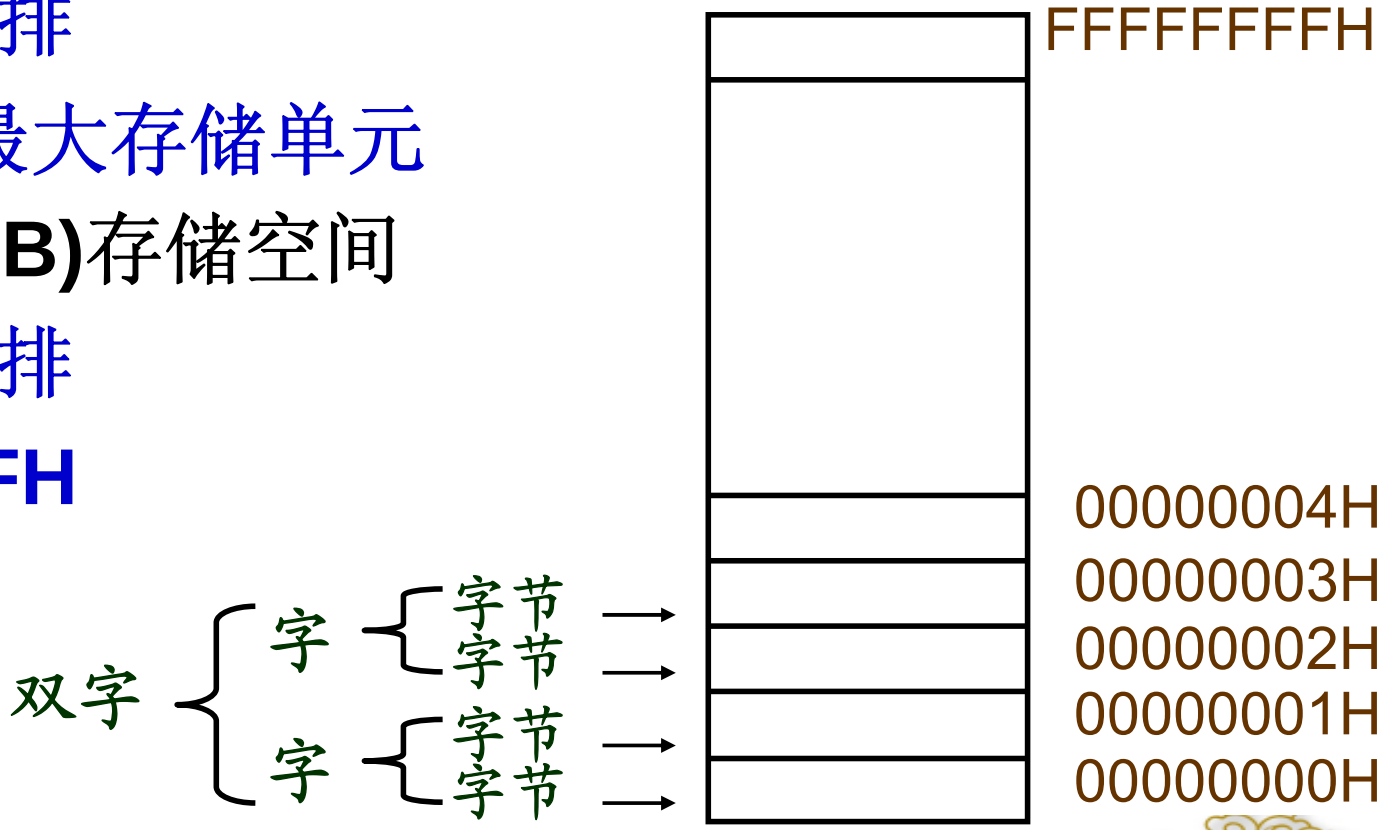
- 主存储器容量很大，被划分成许多存储单元
- 每个存储单元被编排一个号码、即存储单元地址
  - 称为存储器地址（**Memory Address**）
- 每个存储单元以字节为基本存储单位
  - 即字节编址（**Byte Addressable**）
  - 一个字节（**Byte**）等于**8**个二进制位（**Bit**）
  - 二进制位是计算机存储信息的最小单位

数据基本单位：位、字节、字和双字



存储器的物理地址

- 处理器连接的物理存储器使用物理地址
  - 从0开始顺序编排
  - 直到其支持的最大存储单元
- IA-32有4GB(＝2^{32} B)存储空间
  - 从0开始顺序编排
  - 直到FFFFFFFFH



存储模型

- 高性能处理器集成有存储管理单元**MMU**
- 操作系统利用**MMU**进行主存储器空间管理
  - 程序并不直接寻址物理存储器
- **IA-32**处理器提供**3**种存储模型（**Memory Model**）
  - 用于程序访问存储器

MMU：Memory Management Unit

IA-32处理器的存储模型

- 平展存储模型（**Flat Memory Model**）
  - 存储器是一个连续的**4GB**线性地址空间
- 段式存储模型（**Segmented Memory Model**）
  - 存储器由一组独立的地址空间组成：段（**Segment**）
  - 每个段都可以达到**4GB**
- 实地址存储模型（**Real-address Memory Model**）
  - **8086**处理器的存储模型（最大**1MB**）
  - 段式存储模型的特例（段最大**64KB**）

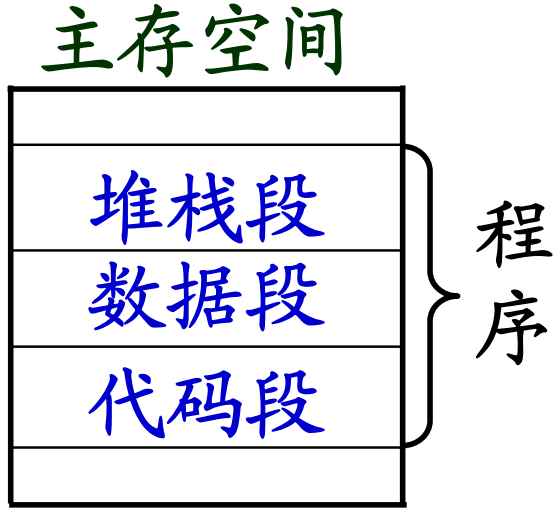
存储空间分段管理

- “段”是保存相关代码或数据的一个主存区域
- 应用程序主要涉及3类基本段
  - 代码段（**Code Segment**）

    存放程序的可执行代码（处理器指令）
  - 数据段（**Data Segment**）

    存放程序所用的数据，例如全局变量
  - 堆栈段（**Stack Segment**）

    程序需要的特殊区域，存放返回地址、临时变量等



逻辑地址（Logical Address）

- 存储器空间可以分段管理，采用逻辑地址指示
- 逻辑地址＝段基地址：偏移地址
  - 段基地址＝在主存中的起始地址
  - 偏移地址＝距离段基地址的位移量
- 处理器内部以及程序员编程时采用逻辑地址

房间编号的比喻：物理地址与逻辑地址

物理地址＝绝对地址：**15**（第**15**号房间）

21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
01	02	03	04	05	06	07	08	09	10

逻辑地址＝相对地址：**205**（**2**层**05**号房间）

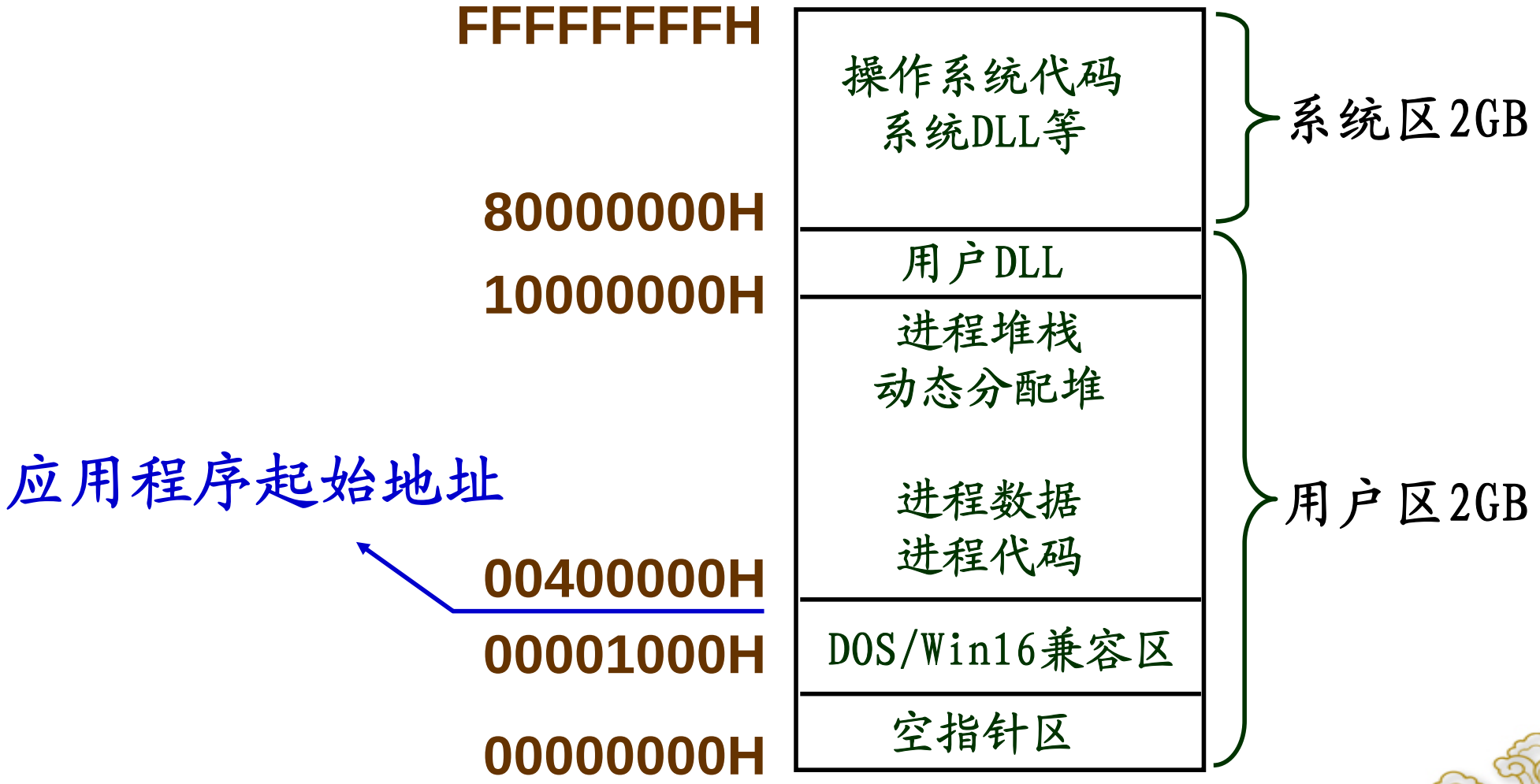
301	302	303	304	305	306	307	308	309	310
201	202	203	204	205	206	207	208	209	210
101	102	103	104	105	106	107	108	109	110

物理地址与逻辑地址的转换

- 程序员编程时采用逻辑地址
- 操作系统利用存储管理单元**MMU**

  将逻辑地址映射为线性地址（虚拟地址）
- 处理器使用物理地址访问主存储器芯片

Win32的虚拟地址分配



处理器专用寄存器

IA-32处理器的常用寄存器

寄存器 { 透明寄存器
可编程寄存器 { 通用寄存器
专用寄存器

通用寄存器	32位通用寄存器	EAX EBX ECX EDX ESI EDI EBP ESP
	16位通用寄存器	AX BX CX DX SI DI BP SP
	8位通用寄存器	AH AL BH BL CH CL DH DL
专用寄存器	标志寄存器	EFLAGS
	指令指针寄存器	EIP
	段寄存器	CS DS SS ES FS GS

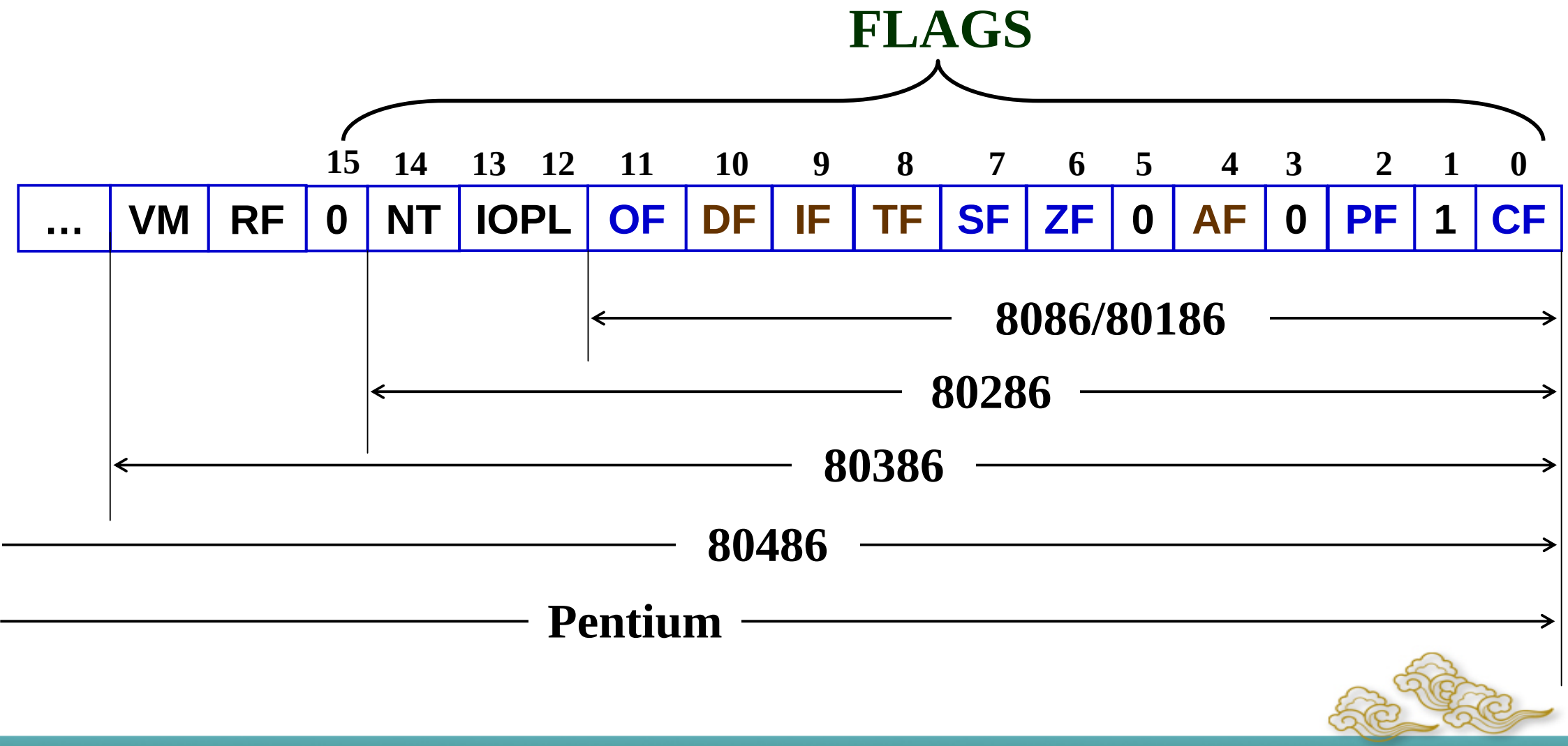
什么是标志（Flag）

- 标志体现了某种工作形态
- 有些处理器标志用于反映指令执行结果
  - 加减是否进借位，数据是否为零、或者是正还是负
- 有些处理器标志用于控制指令执行形式
  - 处理器是否单步操作、是否响应外部中断
- 设计一个或多个二进制位表示一种标志
- 用0和1的不同组合表达标志的不同状态

标志寄存器

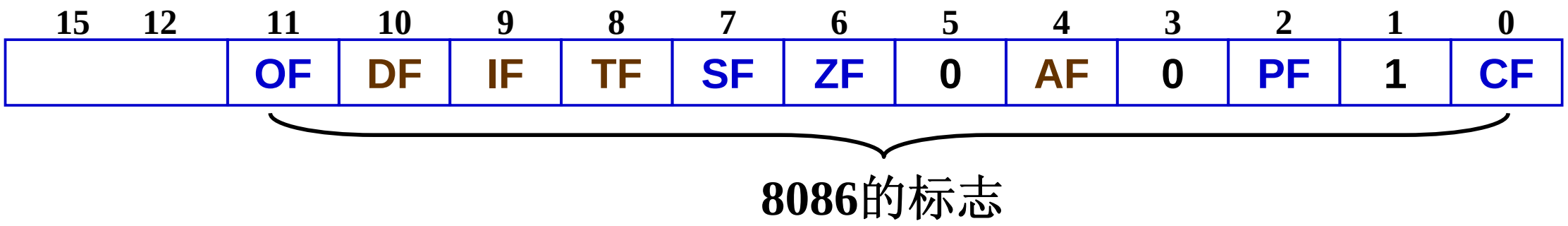
- 各种标志组合在一个专用寄存器形成标志寄存器
- 8086支持16位标志寄存器FLAGS
- IA-32处理器形成32位EFLAGS标志寄存器
  - 状态标志：记录指令执行结果的辅助信息
  - 控制标志：方向标志DF，仅用于串操作指令
  - 系统标志：控制操作系统或核心管理程序的操作方式

标志寄存器EFLAGS



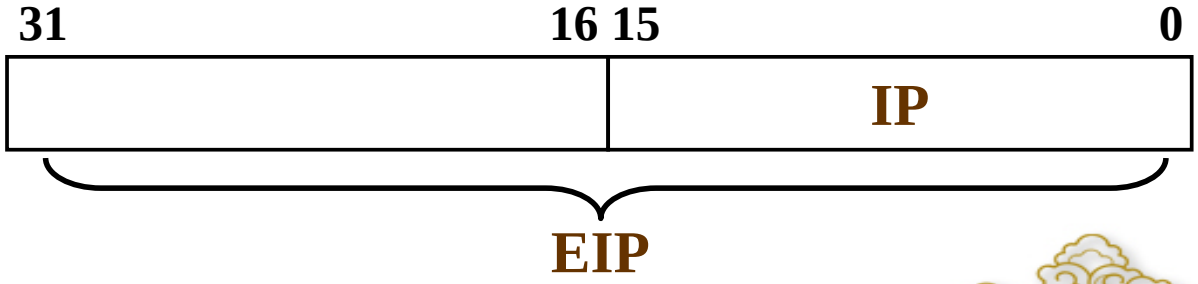
处理器最基本的标志：状态标志

- 用来记录指令执行结果的辅助信息
- 加减运算和逻辑运算指令主要设置它们
- 其他有些指令的执行也会相应地设置它们
- 处理器主要使用其中5个构成各种条件
  - 分支指令判断这些条件实现程序分支



指令指针寄存器EIP

- 保存将要执行的指令在主存的存储器地址
  - 顺序执行时自动增量（加上该指令的字节数）
    指向下一条指令
  - 分支、调用等操作时执行控制转移指令修改
    引起程序转移到指定的指令执行
  - 出现中断或异常时被处理器赋值而相应改变



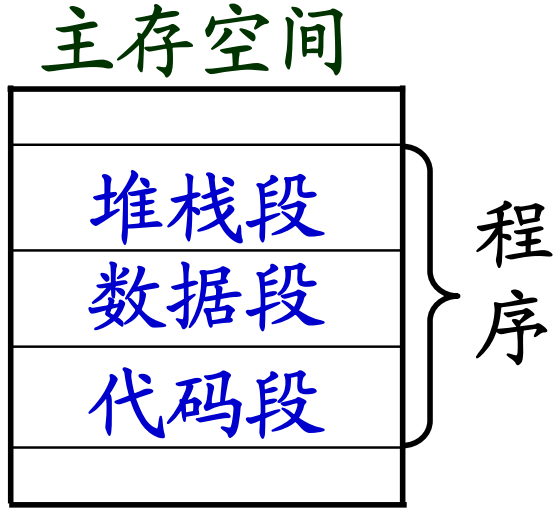
存储空间分段管理

- “段”是保存相关代码或数据的一个主存区域
- 应用程序主要涉及3类基本段
  - 代码段（**Code Segment**）

    存放程序的可执行代码（处理器指令）
  - 数据段（**Data Segment**）

    存放程序所用的数据，例如全局变量
  - 堆栈段（**Stack Segment**）

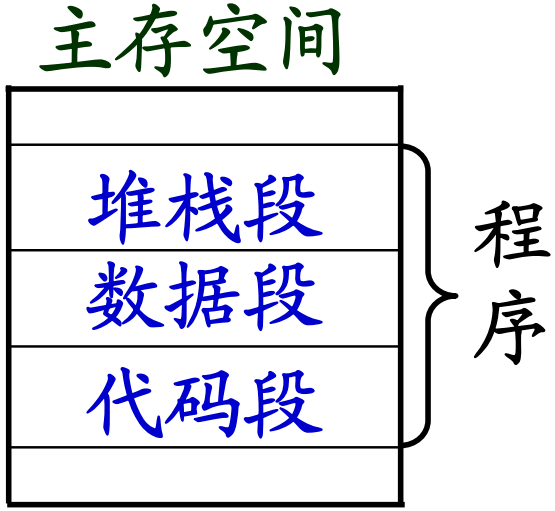
    程序需要的特殊区域，存放返回地址、临时变量等



段寄存器

- 段寄存器表明某个段在主存中的位置
- 6个16位段寄存器：CS　DS　SS　ES　FS　GS

代码段	CS（Code Segment）
堆栈段	SS（Stack Segment）
数据段	DS（Data Segment） ES （Extra Segment） FS GS



代码段的当前指令地址

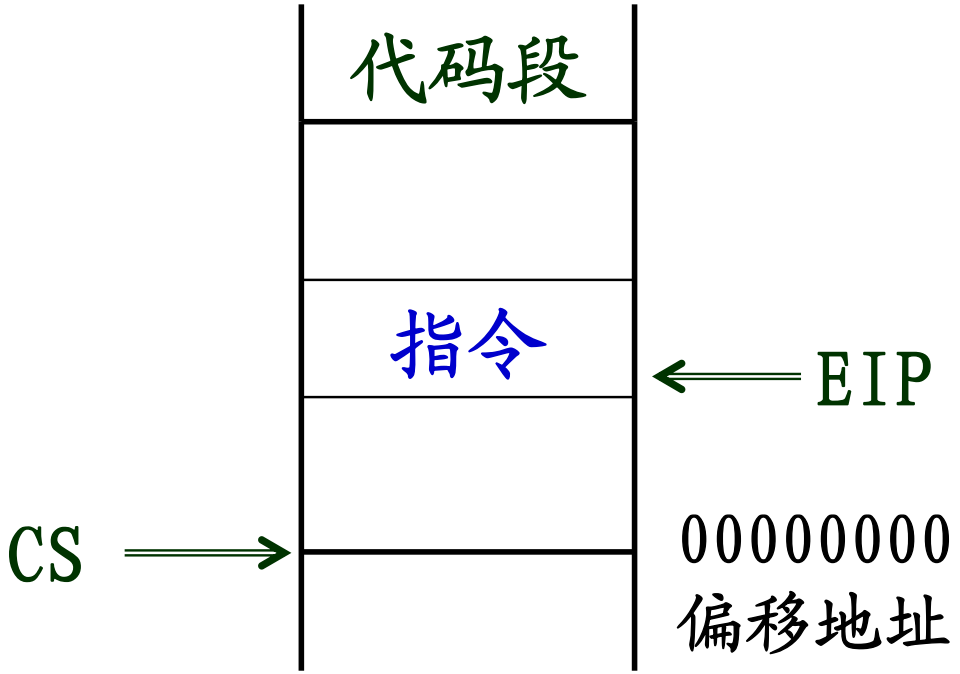
- 代码段（Code Segment）
  - 段基地址

    代码段寄存器CS指示
  - 偏移地址

    指令指针寄存器EIP保存

编程采用逻辑地址

段基地址：偏移地址



堆栈段的当前栈顶地址

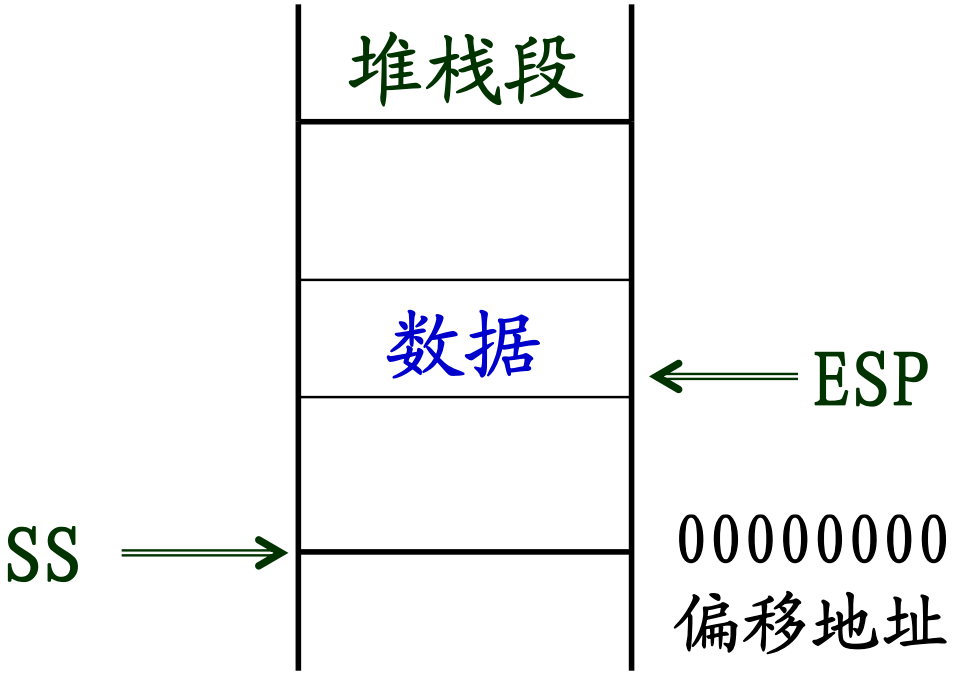
- 堆栈段（Stack Segment）
  - 段基地址

    堆栈段寄存器SS指示
  - 偏移地址

    堆栈指针寄存器ESP保存

编程采用逻辑地址

段基地址：偏移地址



数据段的操作数地址

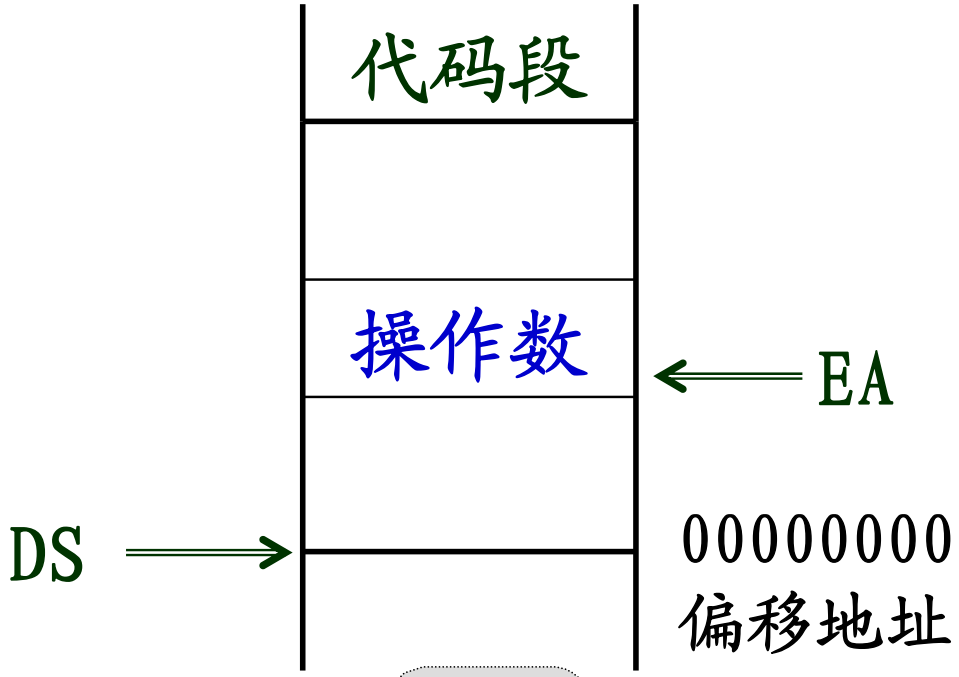
- 数据段（Data Segment）
  - 段基地址

    数据段寄存器DS指示

    有时也用ES、FS和GS指示
  - 偏移地址

    存储器寻址方式计算出

    有效地址EA指示



编程采用逻辑地址

段基地址：偏移地址

IA-32处理器的常用寄存器

寄存器 { 透明寄存器
可编程寄存器 { 通用寄存器
专用寄存器

通用寄存器	32位通用寄存器	EAX EBX ECX EDX ESI EDI EBP ESP
	16位通用寄存器	AX BX CX DX SI DI BP SP
	8位通用寄存器	AH AL BH BL CH CL DH DL
专用寄存器	标志寄存器	EFLAGS
	指令指针寄存器	EIP
	段寄存器	CS DS SS ES FS GS