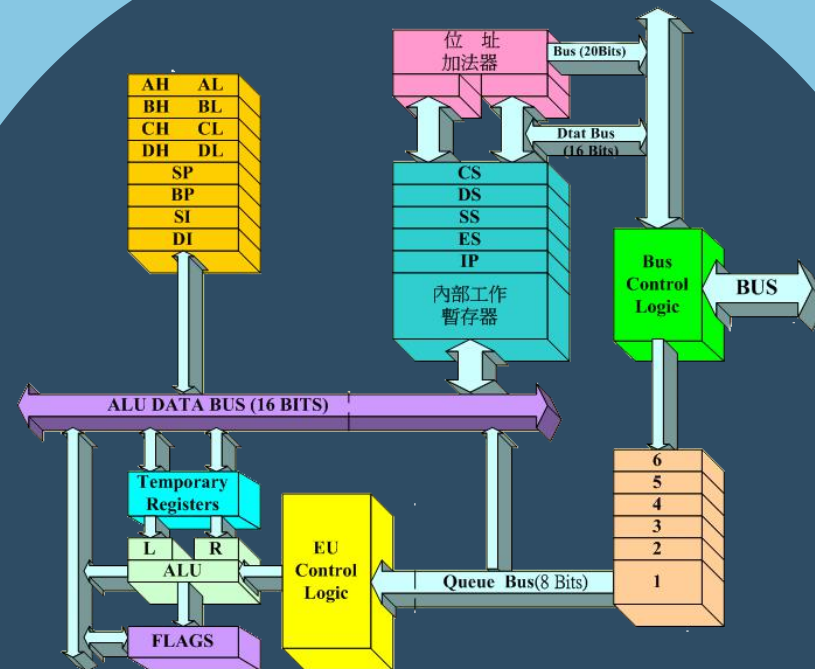


80x86汇编

贺利坚 主讲

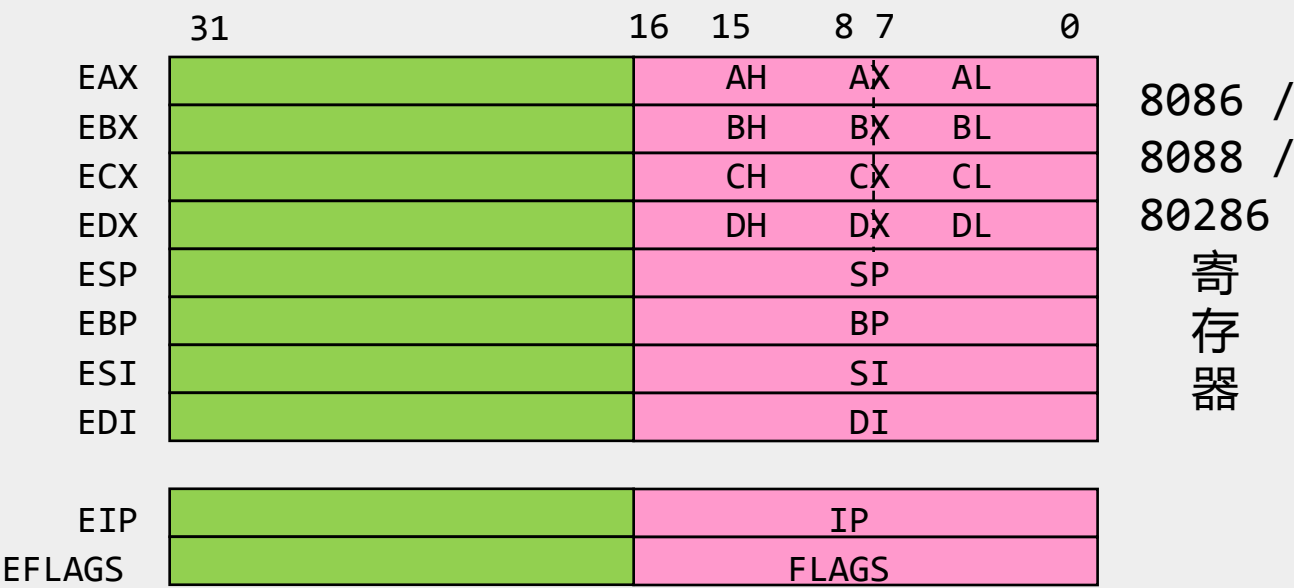


汇编语言程序设计
Assembly Language

80x86 CPU性能一览

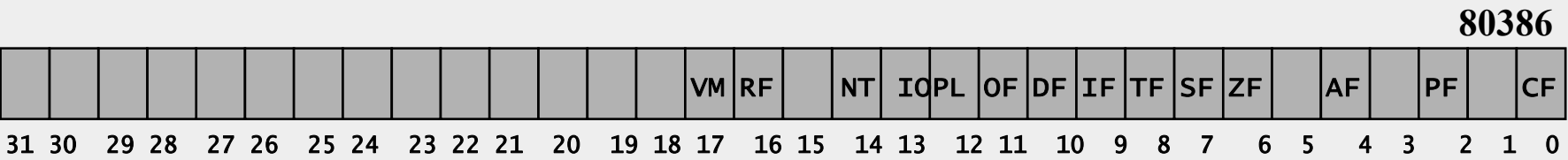
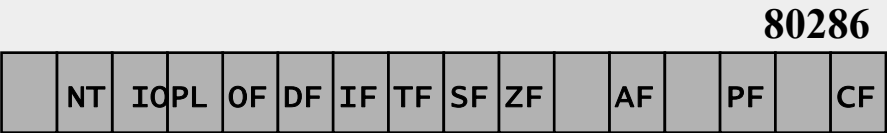
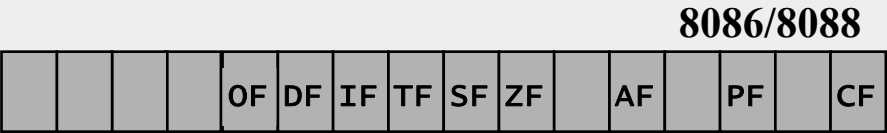
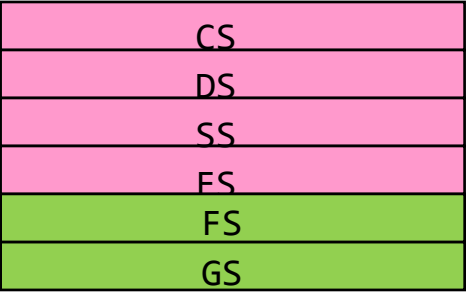
CPU	地址总线 宽度	寻址 能力	数据总线 宽度	一次传送 数据
8080	16	640KB	8	1B
8088	20	1MB	8	1B
8086	20	1MB	16	2B
80286	24	16MB	16	2B
80386	32	4GB	32	4B

80x86的寄存器结构



标志寄存器：由FLAGS到EFLAGS

80x86的程序可见寄存器组
通用寄存器
专用寄存器
段寄存器



80x86的寻址方式

1. 8086的寻址方式

- 立即寻址 `MOV AX, 3069H`
- 寄存器寻址 `MOV AL, BH`
- 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]`

2. 80386新增

- 基址比例变址寻址方式 例：`MOV ECX, [EAX] [EDI*4]`
- 相对基址比例变址寻址方式 例：`MOV EAX, TABLE [EBP] [EDI*4]`


地址成分	16位寻址	32位寻址
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外的任何32位通用寄存器
比例因子	1	1、2、4、8

对于元素大小为2、4、8字节的数组，可以在变址寄存器中给出数组元素的下标，依靠比例因子，将下标转换为变址值。

80x86 的指令系统


(1) 指令集的32位扩展

 所有 16 位指令都可扩展到 32 位 `MOV EAX, 1`

 可使用 32 位的存储器寻址方式 `MOV EAX, [EDX]`










(2) 使用方式的扩展

 `IMUL`：单操作数指令 → 双操作数指令 / 三操作数指令 `IMUL REG, SRC`

 `PUSH`：允许使用立即数寻址方式 `PUSH 36H`

 移位指令：移位次数可用 8 位立即数 (1~31) `SHL EAX, 16`

80x86 新增指令

 MOVSBX	带符号扩展传送
 MOVZX	带零扩展传送
 PUSHA / PUSHAD	所有寄存器进栈
 POPA / POPAD	所有寄存器出栈
 LFS / LGS / LSS	取地址
 PUSHFD	标志进栈
 POPFD	标志出栈
 CWDE	字转换为双字 EAX
 CDQ	双字转换为 4 字 EDX EAX
 BSWAP	32 位寄存器的字节次序变反
 XADD	交换加
 CMPXCHG	比较并交换 (486)
 CMPXCHG8B	比较并交换 8 字节(Pentium)A

 BT	位测试
 BTS	位测试并置1
 BTR	位测试并置0
 BTC	位测试并变反
 BSF	正向位扫描
 BSR	反向位扫描
 SHLD	双精度左移
 SHRD	双精度右移
 INSB / INSW / INSD	串输入
 OUTSB / OUTSW / OUTSD	串输出

条件设置指令

(1) 根据单个条件标志的值把目的字节置 1



SETZ / SETE

SETNZ / SETNE



SETS / SETNS

SETO / SETNO



SETP / SETPE

SETNP / SETPO



SETC / SETB / SETNAE

SETNC / SETNB / SETAE

(2) 比较两个无符号数，根据比较结果把目的字节置 1



SETB / SETNAE / SETC

SETNB / SETAE / SETNC



SETBE / SETNA

SETNBE / SETA

(3) 比较两个带符号数，根据比较结果把目的字节置 1



SETL / SETNGE

SETNL / SETGE



SETLE / SETNG

SETNLE / SETG

Intel系列微处理器的3种工作模式

工作模式	工作特点		
实模式	8086/8088支持的单任务工作模式，优势在于程序可以直接访问系统内存和硬件设备。		
保护模式	程序获得独立的内存段，也会阻止使用自身段范围之外的内存，提供对多任务环境的支持。		
虚拟8086模式	可以从保护模式切换到实模式，提供对原生实模式程序的支持。		

工作模式	8086	80286	80386以上
实模式	√		
保护模式		√	
虚拟8086模式			√