南京大学
NANJING UNIVERSITY

Lab1 系统引导

助教：郑贺

实验内容

- 在实模式下实现一个 Hello World 程序（lab1.1）
  - 在实模式下在终端中打印 Hello, World!
- 在保护模式下实现一个 Hello World 程序（lab1.2）
  - 在保护模式下在终端中打印 Hello, World!
- 在保护模式下加载磁盘中的 Hello World 程序并运行（lab1.3）
  - 从实模式切换至保护模式，在保护模式下读取磁盘 1 号扇区中的 Hello World 程序至内存中的相应位置，跳转执行该Hello World 程序，并在终端中打印 Hello, World!

系统的启动

- BIOS
  - 在 PC 启动时，首先会在实模式下运行 BIOS
  - BIOS 进行系统自检等工作(第一条指令在哪)
  - 完成上述工作后，BIOS 会读取磁盘的 MBR(Master Boot Record，磁盘的 0 柱面，0 磁头，0 扇区的 512 字节)到内存的 0x7C00(被装入的程序一般称为 Bootloader)，紧接着执行一条跳转指令，将 CS 设置为 0x0000，IP 设置为0x7C00，运行被装入的 Bootloader

8086简介

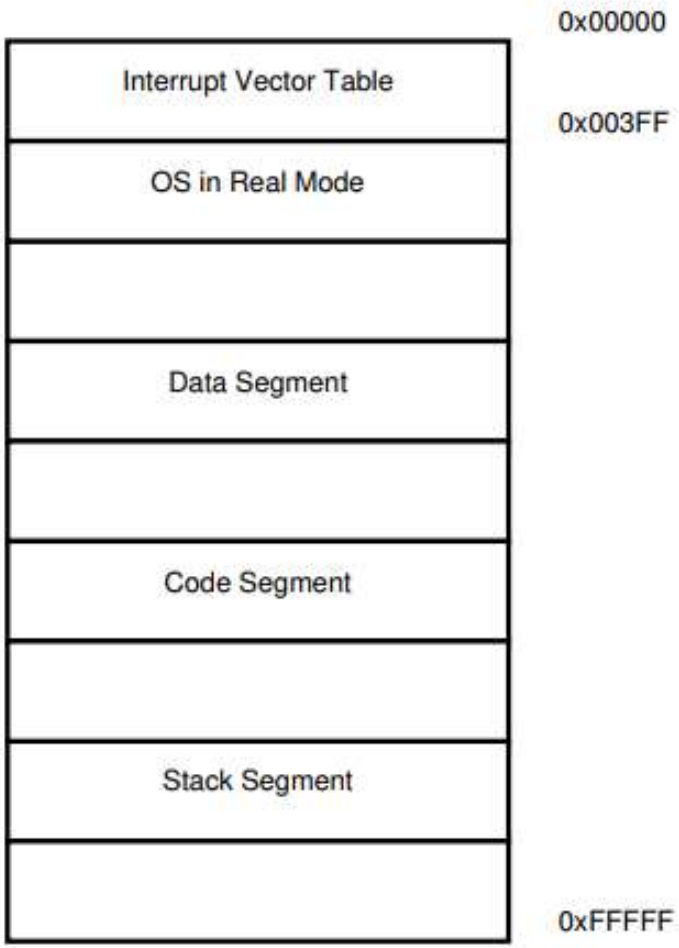
X86 架构的发源地

- 8086 的寄存器集合
  - 通用寄存器(16 位):AX，BX，CX，DX，SP，BP，DI，SI
  - 段寄存器(16 位):CS，DS，SS，ES
  - 状态和控制寄存器(16 位):FLAGS，IP
- 寻址空间与寻址方式
  - 采用实地址空间进行访存，寻址空间为 2^{20}
  - 物理地址 = 段寄存器 << 4 + 偏移地址
  - CS=0x0000:IP=0x7C00 和 CS=0x0700:IP=0x0C00 以及 CS=0x7C0:IP=0x0000 所寻地址是完全一致的

8086简介

- 安全性问题
  - 程序采用物理地址来实现访存，无法实现对程序的代码和数据的保护
  - 一个程序可以通过改变段寄存器和偏移寄存器访问并修改不属于自己的代码和数据
- 分段机制本身的问题
  - 段必须是连续的，从而无法利用零碎的空间
  - 段的大小有限制（最大为 64KB），从而限制了代码的规模

8086简介



- 一个实模式下用户程序的例子
  - 各个段在物理上必须是连续的
  - 装载程序在装入程序时需要按照具体的装载位置设置CS， DS， SS

80386 保护模式

- 保护模式(源自80286)带来的变化
  - 通用寄存器（从 16 位扩展为 32 位）： EAX， EBX， ECX， EDX， ESI， EDI， EBP， ESP
  - 段寄存器（维持 16 位）： CS， DS， SS， ES， FS， GS
  - 状态和控制寄存器（32/64 位）： EFLAGS， EIP， CR0， CR1， CR2， CR3 用于控制处理器的操作模式以及当前执行任务的特性
  - 系统地址寄存器： GDTR， IDTR， TR， LDTR
  - 调试与测试用寄存器： DR0，… ， DR7， TR0， … ，TR7

80386保护模式

	8086 寄存器	80386 寄存器
通用寄存器	AX，BX，CX，DX SP，BP，DI，SI	EAX，EBX，ECX，EDX ESI，EDI，EBP，ESP
段寄存器	CS，DS，SS，ES	CS，DS，SS，ES，FS，GS
段描述符寄存器	无	对程序员不可见
状态和控制寄存器	FLAGS，IP	EFLAGS，EIP CR0，CR1，CR2，CR3
系统地址寄存器	无	GDTR，IDTR，TR，LDTR
调试寄存器	无	DR0，…，DR7
测试寄存器	无	TR0，…，TR7

80386 保护模式

- 寻址方式的变化
  - 在保护模式下，分段机制是利用一个称作段选择子的偏移量到全局描述符表中找到需要的段描述符，而这个段描述符中就存放着真正的段的物理首地址，该物理首地址加上偏离量即可得到最后的物理地址
  - 一般保护模式的寻址可用 0xMMMM:0xNNNNNNNN 表示，其中 0xMMMM 表示段选择子的取值， 16 位（其中高 13 位表示其对应的段描述符在全局描述符表中的索引，低 3 位表示权限等信息）， 0xNNNNNNNN 表示偏移量的取值， 32位
  - 段选择子为 CS， DS， SS， ES， FS， GS 这些段寄存器

80386 保护模式

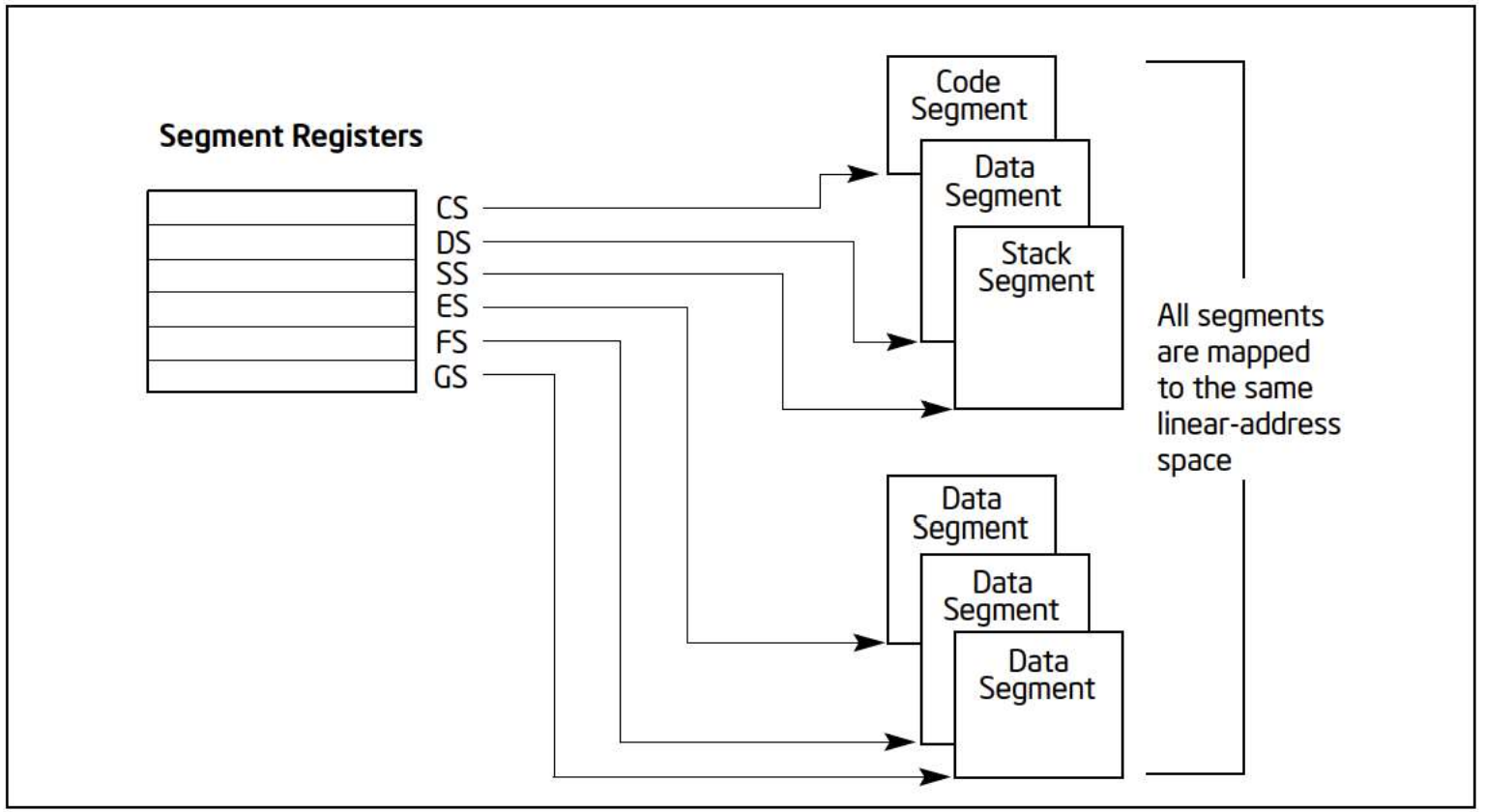
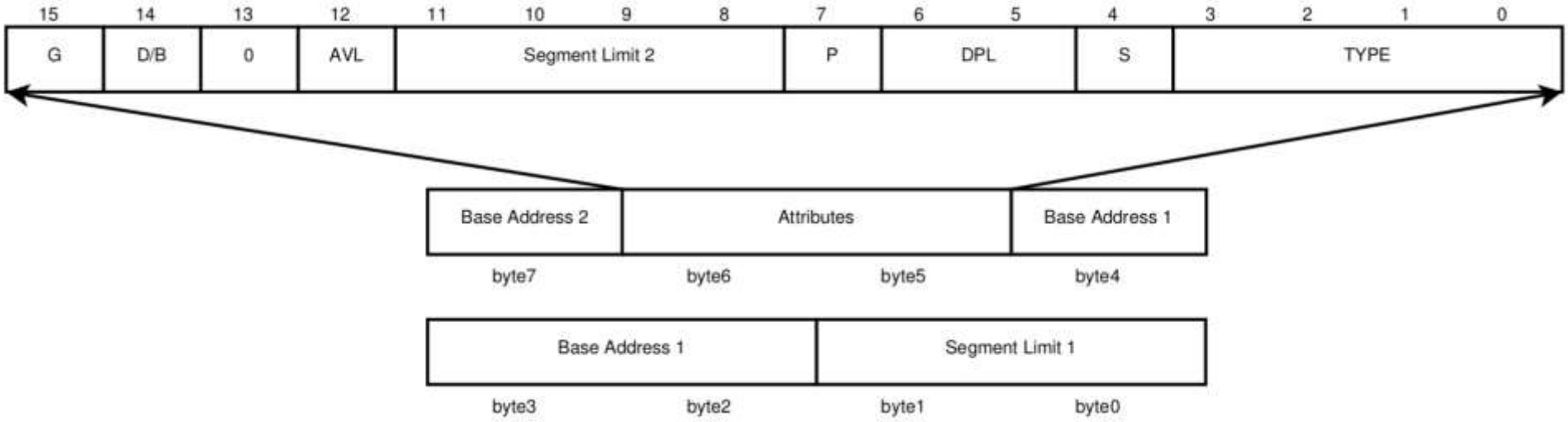


Figure 3-7. Use of Segment Registers in Segmented Memory Model

80386 保护模式

- 段描述符
  - 每个段描述符为 8 个字节，共 64 位
  - 段基址为第 2，3，4，7 字节，共 32 位



80386 保护模式

Intel manual vol3: 3.4.5:
https://cdrdv2.intel.com/v1/dl/getContent/671447

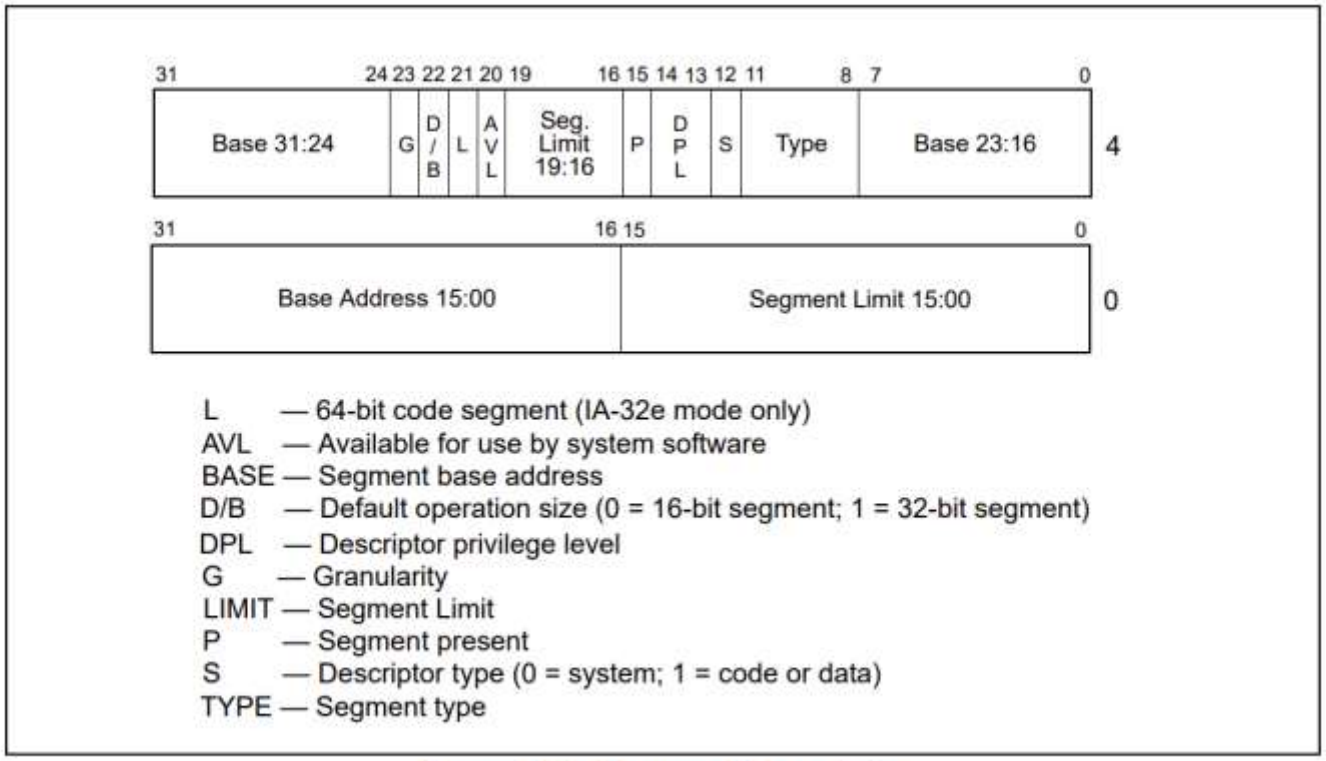
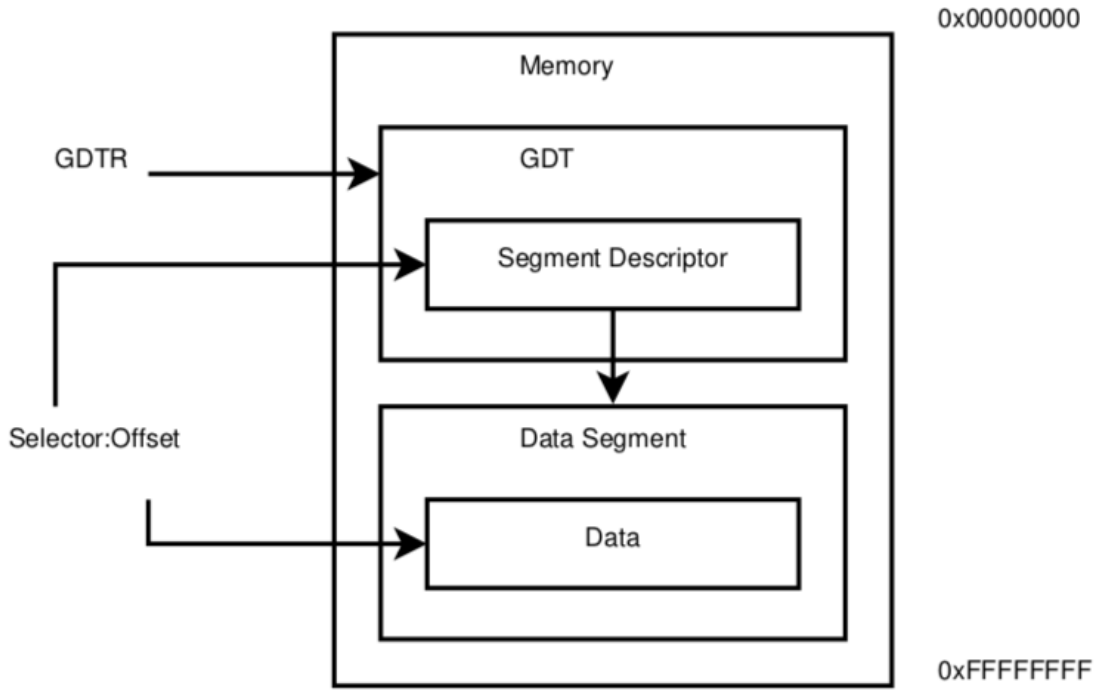


Figure 3-8. Segment Descriptor

80386 保护模式

- 80386 及以后的处理器专门设计了一个寄存器 GDTR (Global Descriptor Table Register)用于存储全局描述符表在内存中的基地址以及其表长界限



从实模式切换到保护模式

- 在实模式下，操作系统需要初始化段表（如GDT）和描述符表寄存器（如GDTR）。在初始化完成后，操作系统通过将0号控制寄存器（CR0）中的PE位置为1的方式，来通知机器进入保护模式。在此之前，CR0中的PE初始化为0。