西安交通大学
XI'AN JIAOTONG UNIVERSITY

第七章 存储器管理

主讲：乔瑞萍

信息与通信工程学院

学习要点

- 掌握实方式存储器管理
  - 分段结构（逻辑地址 → 物理地址）
- 掌握保护方式存储器管理
  - 段、页式两级存储器管理（逻辑地址 → 线性地址 → 物理地址）
- 了解保护及任务切换
- 虚拟8086方式

返回

重点难点

- P273，存储器管理是由微处理器提供的对系统存储器资源进行管理的机制，其目的是方便于软件程序对存储器的应用。
- 80386、80486CPU共有3种工作模式：
  - 实方式；
  - 保护虚地址方式；
  - 虚拟8086方式。

  注：实方式与8086相同。

7.1实方式存储器管理

- 1、段存储器管理
- 2、物理地址的形成
  - （见2.2.3.）

特点：

①P273，实方式下，32位地址总线（80386、80486）中只能使用低20位，其存储空间和8086/8088一样，只有1MB。

（所谓存储空间是指能够用来访问存储器的所有有效地址的集合）

②实方式下，不实施保护机制，P273

③存储器管理采用分段结构，解决16位寄存器对20位物理地址的表示。

1、段存储器管理

- 段存储器完成逻辑地址向物理地址的转换
- 8086 CPU不支持虚拟存储管理

2、物理地址的形成

逻辑地址

- 定义：以段地址和偏移地址形式表达的某存储单元地址，称之。实际上是编程地址。
- 表示格式：段地址：偏移地址
  - 例：8000H：0100H

物理地址

- 定义：存储单元实际地址编码。即20位二进制表达的存储单元的唯一地址。

两者关系：物理地址=段地址×10H＋偏移地址

特点：

- 一个存储单元的物理地址是唯一的，而其逻辑地址不是唯一的。（段地址和偏移地址有多种组合）
- 当80286以上的CPU工作于实方式时，其存储器管理与8086/8088CPU相同。

返回

7.2保护方式存储器管理

- 1、若将CR_0控制寄存器PE位置位，80386便工作于保护虚地址方式。其与实方式存储器管理区别：
- 1）保护方式向程序员提供了额外的工具用来进行段尺寸的扩充和使用上的限制，从而实现了对存储器访问的保护机制。
- 2）保护方式下的分段机制与实方式的有很大的不同，并且保护方式寻址引入了虚拟存储器概念。

构造虚拟存储器的动机：

- 1.允许云计算在多个虚拟机之间有效而安全地共享存储器；
  - 为了允许多个虚拟机共享同一个存储器，我们必须在虚拟机之间进行保护；
  - 每个程序都编译到它自己的地址空间；
  - 虚拟存储器实现程序地址空间到物理地址的转换。
- 2.允许单用户程序使用超过主要存储器的容量。
  - 程序对存储器太大，程序员要将其变成合适的大小（划成互斥的段：装入、换出）

3.存储容量需求

- 应用需求
  - 海量数据处理
    - 大数据、天气预报、地震预测、石油勘探、搜索
  - 多媒体信息处理
    - 语音、图形、图像
- 软件需求
  - Nathan软件第一定律：软件是一种可以膨胀到充满整个容器的气体。
- 技术需求
  - 多进程、多道程序

给程序员一个大容量、可管理的编址空间

4.提高存储器容量

- 降低主存储器成本，在同样成本下，可以获得更大的主存容量
  - 主存的价格到今天也依然比较昂贵
  - 程序对主存的“胃口”的增加和主存价格的降低速度几乎同样的快
- 采用虚拟存储器
  - 只在确实需要的时候才把程序和数据装入到主存中
    - 交换的粒度
    - 地址转换
    - 共享及保护

（注：3、4摘自清华大学“计算机组成原理”课件）

- 大多数的虚拟存储管理使用三级地址空间：逻辑地址、线性地址和物理地址
- 物理地址：主存储器的地址。
- 保护：一组确保共享处理器、主存、I/O设备的多个进程之间没有故意地、无意地读写其他进程的数据机制，这些保护机制可以将OS和用户的进程隔离开来。

2、虚拟存储器技术

- 将主存和辅存的一部分统一编址，看作一个完整的虚拟存储空间。正在使用的虚拟存储器被置入主存（实存），暂时未使用的则保存在辅存中。从80386开始内置了MMU，用硬件和软件相结合的方法完成虚存和实存之间的调度。

即虚拟存储器由存储器管理机制和一个大容量快速硬磁盘支持。

7.2.1存储器的分段管理

32位机采用片内两级存储管理，即分段和分页管理。

- 7.2.1 存储器的分段管理
- 7.2.2 存储器的分页管理

返回

1、存储器的分段管理

- P275，无论是实方式还是保护方式，编程都只与逻辑地址打交道。逻辑地址的表达方式是：段地址：偏移量
- 在实方式下：
  - 段地址是段起点物理地址（20位地址中最低4位为0）的高16位，
  - 偏移量是段内单元相对于段起点的16位偏移量（距离，以字节为单位）。
  - 程序寻址时，段地址在16位寄存器CS、DS、SS、ES中（这时它们被称为段寄存器），偏移量由指令中的寻址方式确定；
  - 一个段最长为64KB；逻辑地址与物理地址有着直接的数学关系；

- 在保护方式下：
  - 逻辑地址由16位段选择器CS、DS、SS、ES、FS、GS加上偏移地址构成；
  - 寄存器CS等中不再直接是段起点的地址，但通过它可以间接地提供段起点的地址。
  - 这时的逻辑地址又常称为虚拟地址。

P277，段选择器格式。

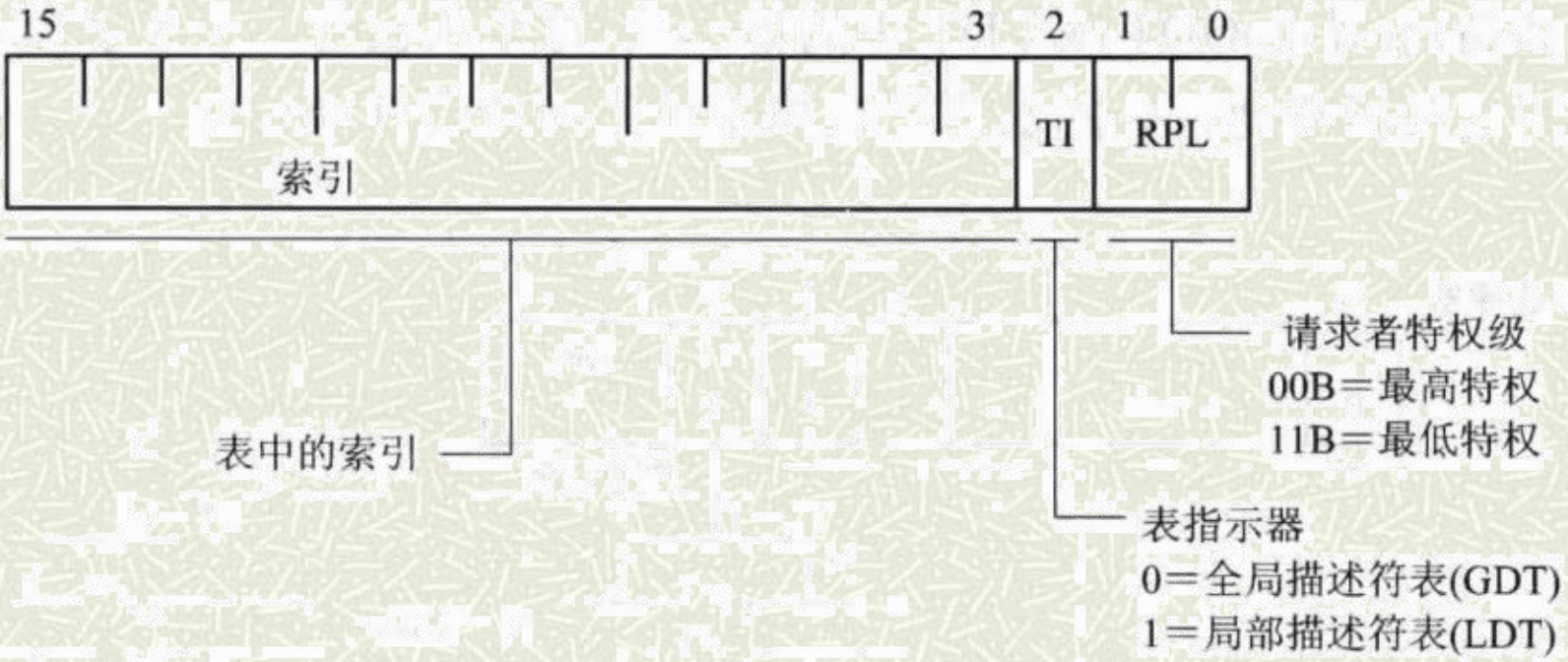


图 7.4　保护方式段选择符格式

- 为了理解分段管理，必须搞清楚：
  - 段的种类；
  - 段描述符；
  - 描述符表；
  - 描述符的选择符；
  - 以及系统地址寄存器。

- 1、保护方式下的段分类
- 2、段选择器
- 3、段描述符
- 4、段描述符表

返回

1、保护模式下段的分类

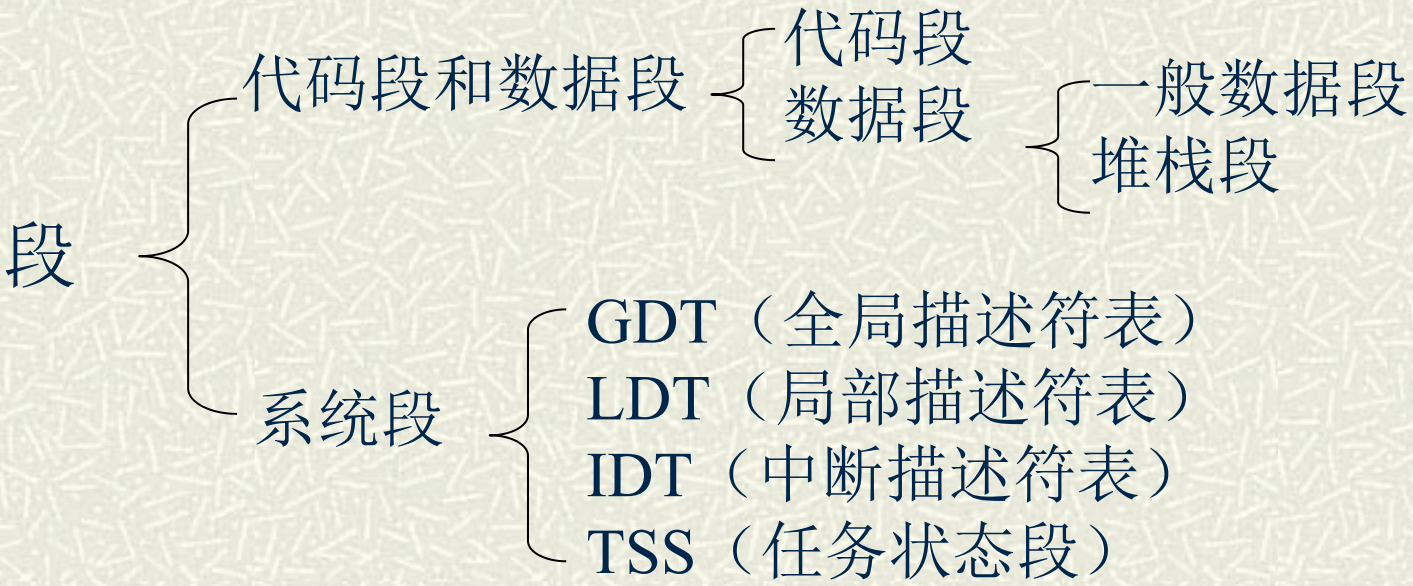


图7.1 保护模式下段的分类

存储器的分段管理是指

- 任何信息都定义在某一段中，通过选择符，可以找到它对应的段描述符，从段描述符中可取出该段的基地址、段的长度和关于该段的其它信息。
- 存储器的寻址（在指令中体现出来的）

  等效成**段择选符**和**偏移地址**两部分，其中选择符间接地给出段的基地址。(见P276图7.3)

段式存储管理的实现

- 设置段表进行管理
  - 段表基地址
  - 段起始地址
  - 段长
  - 装入位
  - 保护、共享等标志

保护方式下分段机制

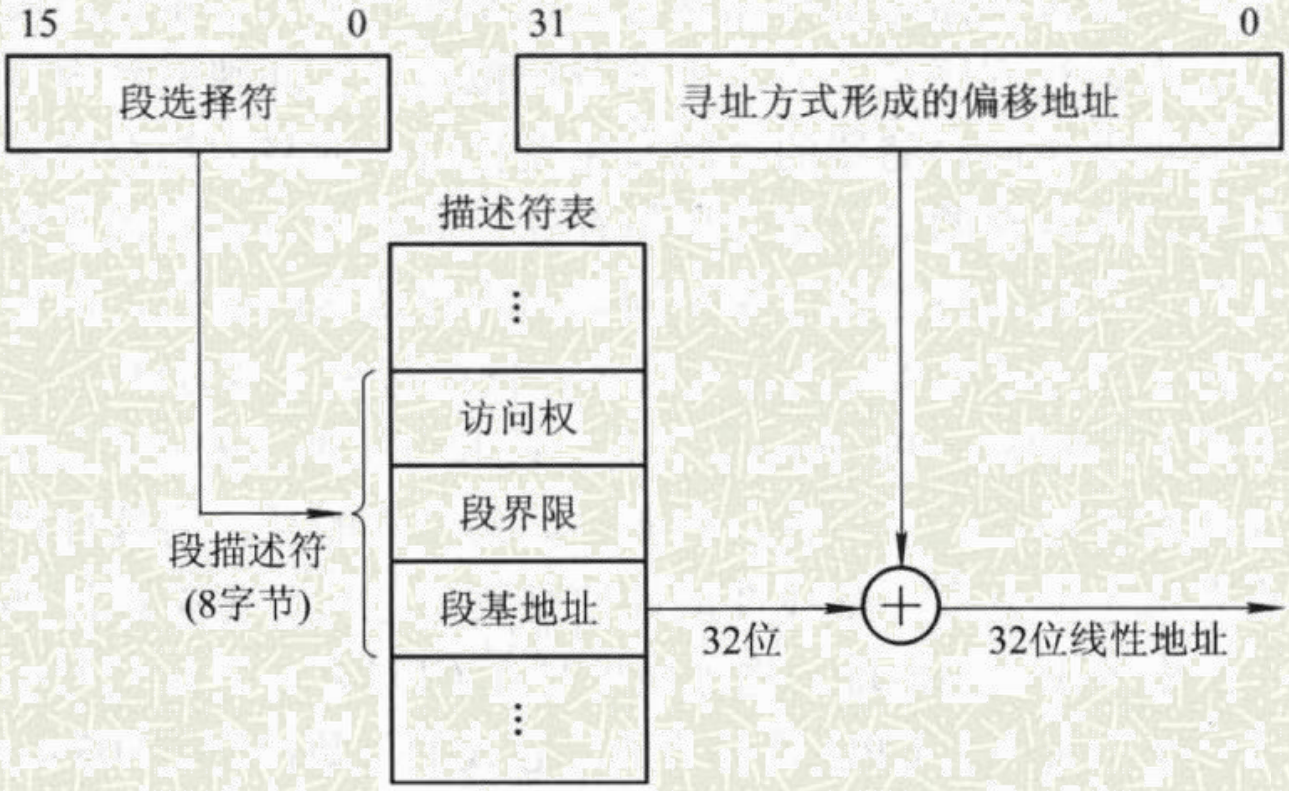


图 7.3　保护虚地址下 80386/80486 的分段机制

- 虚拟地址分段中的段选择器与实方式一样为16位段寄存器：CS、DS、ES、SS，增加FS和GS。
- 有效地址偏移量与实模式一样，根据指令中操作数的寻址方式确定。

返回

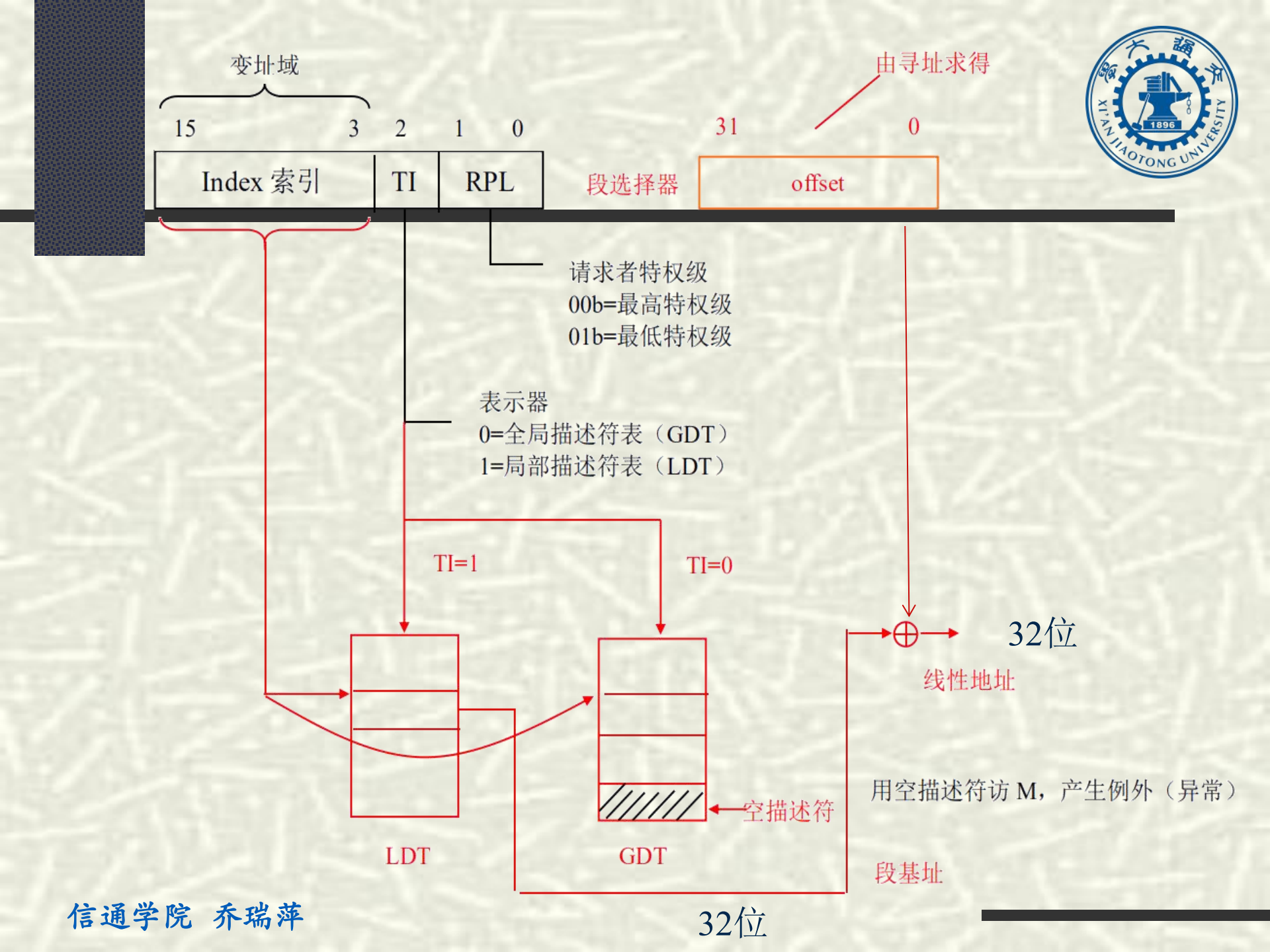
2、段选择器

- 保护方式下，段选择器是一个指向操作系统定义的段信息的指针，可间接地提供段的基地址。

- 介绍几个基本概念：

- 1）全局地址空间：用来存放运行在系统上的所有任务使用的数据和代码段。如：操作系统服务程序、通用库、运行时间支持模块。
- 2）局部地址空间：用来存放一个任务独自占有的特定程序和数据。

- 3）任务：一个单个的、连续的执行线程。
- 4）变址域：用来指向全局地址空间或局部地址空间中以段基地址起始的表中的一项。
- 5）段选择器的高14位用来确定存储器中的一个段，在保护方式下可访问2^{14}个段，扩大存储空间。
  - ①80286：偏移量为16位，每个段最大为2^{16}（64KB），可提供虚拟存储空间为$2^{14}\cdot 2^{16}=2^{30}$（1GB）。
  - ②80386/80486：偏移量为32位，每个段最大为2^{32}（4GB），可提供虚拟存储空间为$2^{14}\cdot 2^{32}=2^{46}$（64TB）。


变址域
15
3
2
1
0
Index 索引
TI
RPL
段选择器
由寻址求得
31
0
offset
请求者特权级
00b=最高特权级
01b=最低特权级
表示器
0=全局描述符表（GDT）
1=局部描述符表（LDT）
TI=1
TI=0
32位
线性地址
用空描述符访 M，产生例外（异常）
空描述符
LDT
GDT
段基址
32位

3）段描述符

- 定义：描述了处理器访问段时段所需要的信息（段信息）主要包括线性存储空间中段的基址和界限，以及有关段的状态和控制信息。32位机把每个段的信息放入一个数据结构中，称作段的描述符。
- 用途：操作系统用段描述符来管理段并利用其将虚拟地址转换成线性地址。

3）分类：分为段描述符和门描述符，

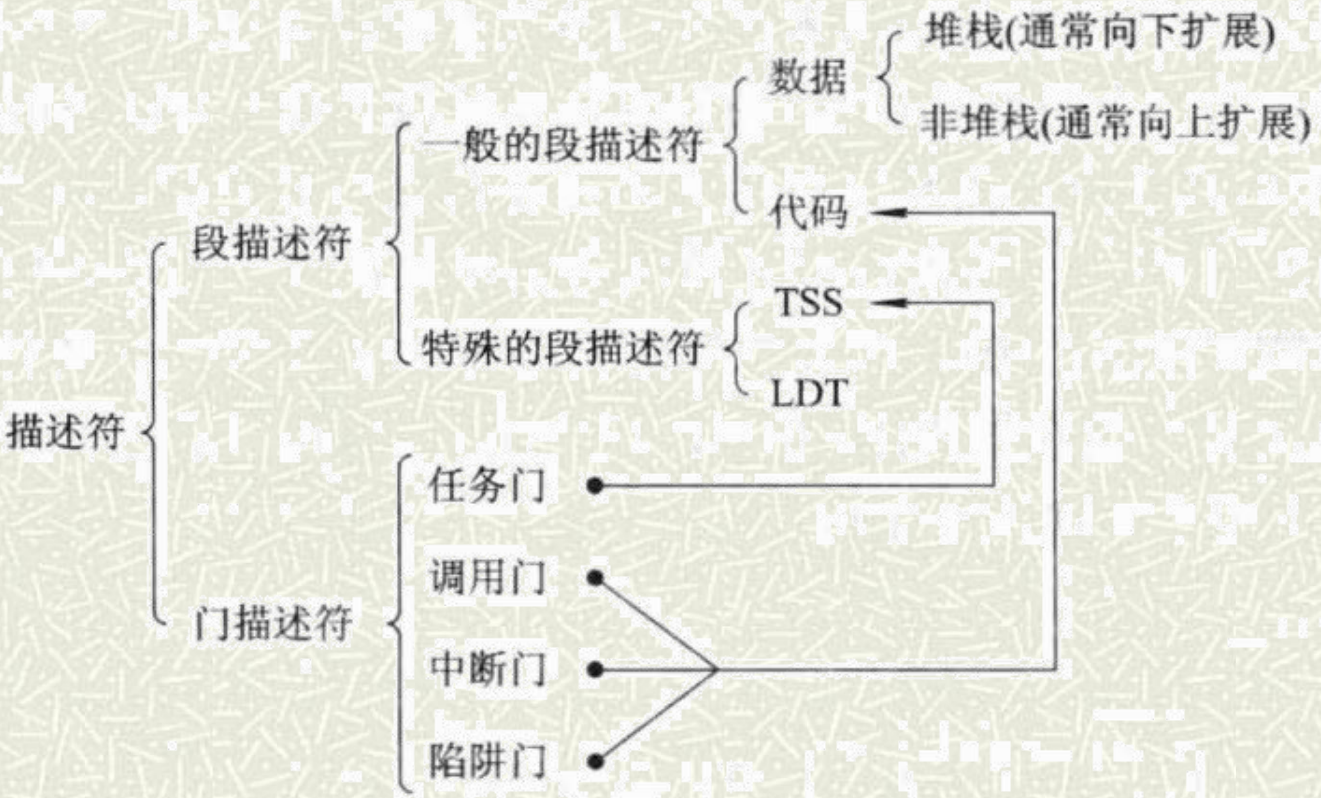
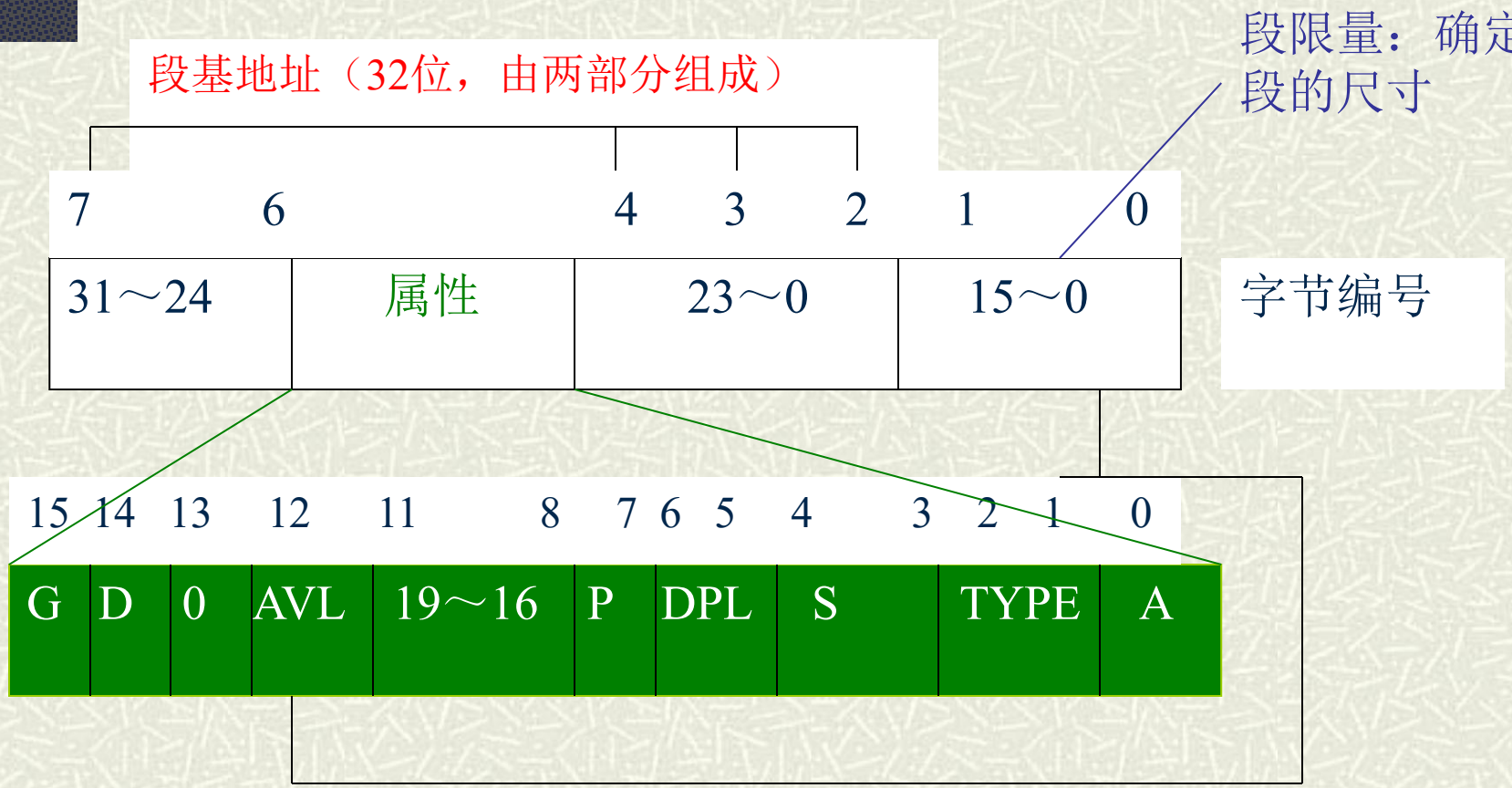


图 7.6　描述符的分类

- 所谓门（GATE）是一种关卡，用来控制从一段程序到另一段程序或从一个任务到另一个任务的转换。在转换过程中自动进行保护检查，并控制转换到目的程序入口。
  - 中断门和陷阱门主要用于正在执行的任务进行中断处理，所以必须设置在IDT中；
  - 任务门用于任务之间的转换控制，例如使用CALL或JMP指令进行任务转换时，需访问GDT或LDT。
- 所有描述符都是由8个字节组成，其中第5～6字节称为访问权字节或属性字节，依次可以确定描述符的类型，并依次组成不同的描述符表。

P279，图7.7程序段描述符格式。



Ⅰ）段基地址：32位，线性空间中段的开始地址。

Ⅱ）段限量：20位，段内可以使用的最大偏移量，指明段的长度（与粒度G共同确定1B~1MB——G=0字节；4KB~4GB——G=1页4KB）。

（字节0、1和字节6的低四位）

Ⅲ）段属性：包括可读出或写入段的特权级等。

① 描述符类型位S：=1，一般段描述符；=0，系统段描述符或门描述符；

② 类型TYPE，P280图7.8，用来定义段的可读/写类型，可执行类型等，不详细介绍。

③ DPL：指出对应段的保护级，从高到低可为0～3级。用来防止一般用户程序任意访问操作系统的对应段。

④ P，存在位，P280，用于虚拟存储技术的实现；

… …

4)段描述符表

- 存储在存储器中的数据结构。保护方式下分为GDT、LDT。
- 描述符表有3种，由描述符顺序组成，占内存一定地址空间区域，由系统地址寄存器（GDTR、LDTR、IDTR）指示其在物理存储器的位置和大小。这3种描述符表分别是全局描述符表GDT、局部描述符表LDT、中断描述符表IDT。
- 史新福，P139，LDT中登记有堆栈段、普通的数据段、代码段、任务门与调用门。IDT中登记有任务门、中断门与陷阱门。GDT中除中断门与陷阱门以外，可登记全部项目。

GDTR、LDTR的格式见P281图7.10，及它们与GDT、LDT的关系P282图7.11。

注意：

①GDT和IDT都只有一个，它们的位置直接由GDTR、IDTR指定；

②而LDT有多个，每个LDT也是一个段，每个LDT又有自己的描述符，称LDT描述符（属于系统段描述符），即描述符表描述符。

③每个LDT描述符是GDT中的一项，所以LDT的定位需要两步：根据当前LDTR中的16位选择器中的13位在GDT中找到对应的LDT描述符，获取它的地址信息，装入LDTR高速缓冲寄存器中。

图 7.10　描述符表寄存器

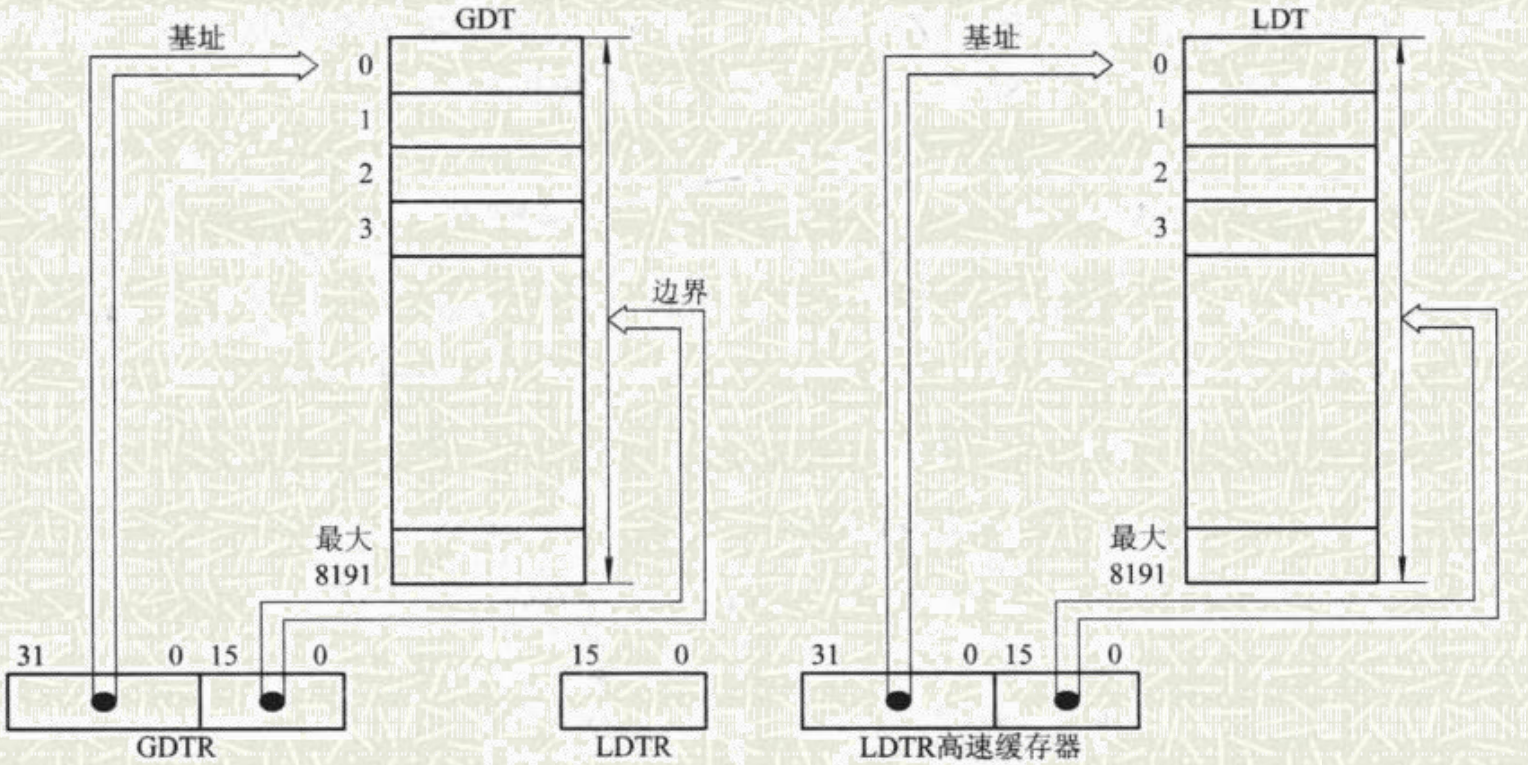


图 7.11　GDTR、LDTR 与描述符表的关系

- 采用描述符表带来如下优点：

- 1）可以大大扩展存储空间。
- 2）可以实现虚拟存储
- 3）可以实现多任务隔离

返回

7.2.2 存储器的分页管理

- 1、分页管理实质
- 2、地址变换
- 3、页转换高速缓冲存储器TLB

返回

内存分页的基本思想:

内存分页管理实现了在小内存上运行大程序，极大地节约了内存设置的费用。

1、分页管理实质

- 把线性地址空间（虚拟）和物理地址空间（实际）都看成由页组成，且线性地址空间中的任何一页均可映射到物理地址空间的任何一页。
- 页是使用存储器中固定尺寸的小块，32位机中规定一页是在线性存储器中连续的4KB区域，并且它的起始地址总是安排在低12位地址信号为0的线性地址处，即能被1000H整除的地址处

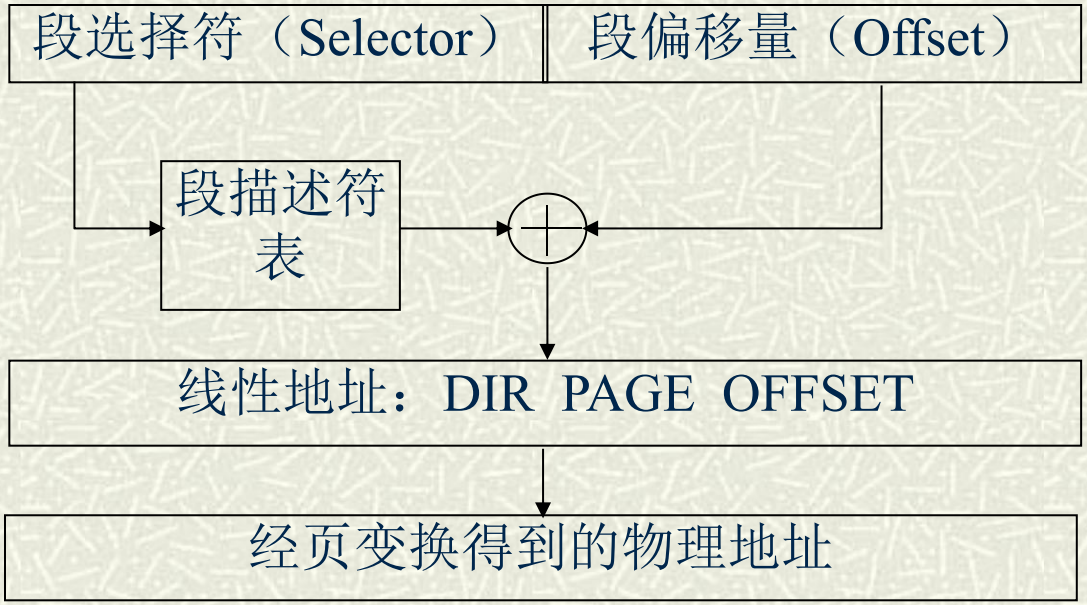
- 分页与分段的主要不同是，一个段的长度可变，而页则是使用存储器中固定尺寸的小块。

返回

2、地址变换

- 1）虚拟地址：保护模式下，虚地址仍由程序指明段选择符和偏移地址两部分表示。
- 2）线性地址：段的基地址与偏移地址之和称为线性地址。由于段的基地址与偏移地址都是32位，所以线性地址也是32位。

- 3）物理地址：就是存储单元的实际地址编码。



- 4）地址变换分为如下几个步骤：
  - ① 有效地址
  - ② 线性地址
  - ③ 物理地址

返回

① 有效地址

- 32位机在执行每条指令期间，硬件将自动地进行复杂的地址计算。寻址机构计算出有效地址。除立即数外，有效地址均按下式计算：

- 有效地址=基址+变址×比例因子+位移量

返回

② 线性地址

- 分段部件将逻辑地址转换为线性地址
- 线性地址=段地址+有效地址
- 段地址是通过段选择符，找到其对应的段描述符，从段描述符中取出之。

返回

③ 物理地址

- 当禁止分页时，物理地址就等于线性地址。当允许分页时，线性地址（32位）分为页目录（10位）、页表项（10位）及偏移量（12位）。分页部件用页目录项表和页表实现地址变换，将线性地址转换为物理地址。

举例

- 物理地址=F（线性地址）
- 其中F（）运算称为页变换。

返回

3、页转换高速缓冲存储器TLB

- 页表存放在内存中，程序访存至少需要两次：1.先获得物理地址；2.获得数据
- 分页结构为实现从线性地址到物理地址的转换，要两次查询内存中的表（页目录表和页表），这样做耗费CPU较多的时间。为解决此问题，有两种方法：

3、页转换高速缓冲存储器TLB

- 1）将这两类各含1024项的表全放在高速缓冲器中，代价昂贵；
- 2）因每个程序所用的存储单元都局限于内存的某个区域，而不会分布于整个地址空间，所以采用**TLB**。

TLB就相当于记录目录中的一些书的位置的小纸片；我们在纸片上记录一些书的位置，并且将小纸片当成图书馆索书号的Cache，这样就不用一直在整个目录中搜索了。

3、页转换高速缓冲存储器TLB

- 快表（Translate-Lookaside Buffer，TLB）：
  - 用于记录最近使用地址的映射信息的高速缓存；
  - 可以避免每次都要访问页表。
- TLB中存放了共32个最近使用过的页表项，通过OS跟踪来控制这些项的保持和更新。32个页表项和每个页面4K字节结合起来可以覆盖128K字节的存储空间。

TLB

- 为页表设置的专用Cache，高效实现虚页号到实页号的转换
- 多路组相联、全相联
- 容量较小，128~256个表项

虚拟存储器管理小结：

- 扩大了程序可访问的存储空间
- 便于实施多任务的保护和隔离
- 便于操作系统实现内存管理

集成虚拟存储器、TLB和cache

- 虚拟存储器和cache系统就像一个层次结构一样共同工作，因此除非数据在主存中，否则，它不可能在cache中出现；
- OS帮助管理该层次结构，当其决定将某一项移到磁盘上去时，就在cache中将该页中的内容刷新。同时，OS修改页表和TLB，而后尝试访问该页上的数据都将发生缺页；
  - 在最好的情况下，虚拟地址由TLB进行替换，然后被送到cache，找到相应的数据，取回并送入处理器。
  - 在最坏的情况下，访问在存储器层次结构的TLB、页表和cache这三个部件中都发生缺失。

虚存与Cache的比较

虚存

- “主存—辅存层次”主要目的是实现存储管理，并帮助解决存储容量的问题。
- 单位时间内数据交换次数较少，但每次交换的数据量大，达几十至几千字节。

Cache

- Cache主要目的是解决存储速度问题，使存储器的访问速度不太影响CPU的运行速度
- 单位时间内数据交换的次数较多，每次交换的数据量较小，只有几个到几十个字节

虚存与Cache的不同

- 虚拟存储器
  - 克服存储容量的不足
  - 获得对主存储器管理的便利
  - 由操作系统管理
- 高速缓冲存储器
  - 解决主存储器与CPU性能的差距
  - 获得最小粒度的访问
  - 由硬件实现

7.3保护及任务切换（自学）

1、保护功能

32位机支持两个主要的保护类型。

- 1）不同任务之间的保护
- 2）同一任务内的保护

2、任务转换

返回

不同任务之间的保护

- 通过给每一个任务分配不同的虚地址空间，而每一个任务有各自不同的虚拟—物理地址转换映射，因而可实现任务之间的完全隔离。

返回

同一任务内的保护

- 在一个任务内定义4种执行特权的级别（0~3）。
- 特权级的保护功能的核心是对段的保护，遵循如下原则：
- 1）不允许从特权级高的代码段向特权级低的代码段控制转移。

- 2）特权级低的代码段在运行时不允许访问特权级高的数据段。
- 3）允许特权级低的代码段向特权级高的代码段控制转移和转移后返回到原来特权级低的代码段。但是在控制转移和返回的两种操作中，都要进行堆栈段的更换，使堆栈段的特权级保持与当时代码段特权级相同。

- 段的改变体现在对段寄存器内选择符的修改上。检查选择符的RPL、CS中的CPL以及选择符对应的段描述符中的DPL三者之间的关系，看其是否满足段的保护规则。

返回

任务转换

- **任务转换的方法如下：**
- 1）JMP/CALL指令，进行直接或间接任务转换。
- 2）IRET/IRETD指令（NT位=1），仅进行直接任务转换。
- 3）中断/异常，仅进行间接任务转换。

返回

7.4虚拟8086方式（自学）

- 虚拟8086方式，实际上就是运行在保护环境中的8086方式，其支持保护机制，也支持分页式内存管理，并可以进行任务切换，但同时又与8086兼容，内存寻址空间为1MB，段地址计算仍然和8086一样。

返回

本章重点与难点

- 存储器分页管理是通过内部寄存器和两级页表来实现的。将内存每4KB划分为一页，每1024页为一个低级管理单位。
- 每页有一个起始地址（低12全0），1024页的起始地址集中排列存放，构成一个页表，页表中的每一项是4个字节，其结构见图7.15（除页其始地址外，还有一些与页相关的特性位）；
- 4GB内存空间，可分成2^{20}个页，应有1024个页表。每个页表本身是一页，可放在内存中的任何地方，它们的起始地址也集中排列存放，构成一个页目录表。页目录表的位置由控制寄存器CR3的高20位加12个0决定。

本章重点与难点

例题

- 设线性地址为25674890H，如何通过页组目录项表和页表将其转变为物理地址。

  设CR3中值为28345XXXH；访问页组前，内存中已有5页被访问过并已定位；访问此页前，内存已有60页被定位。

返回

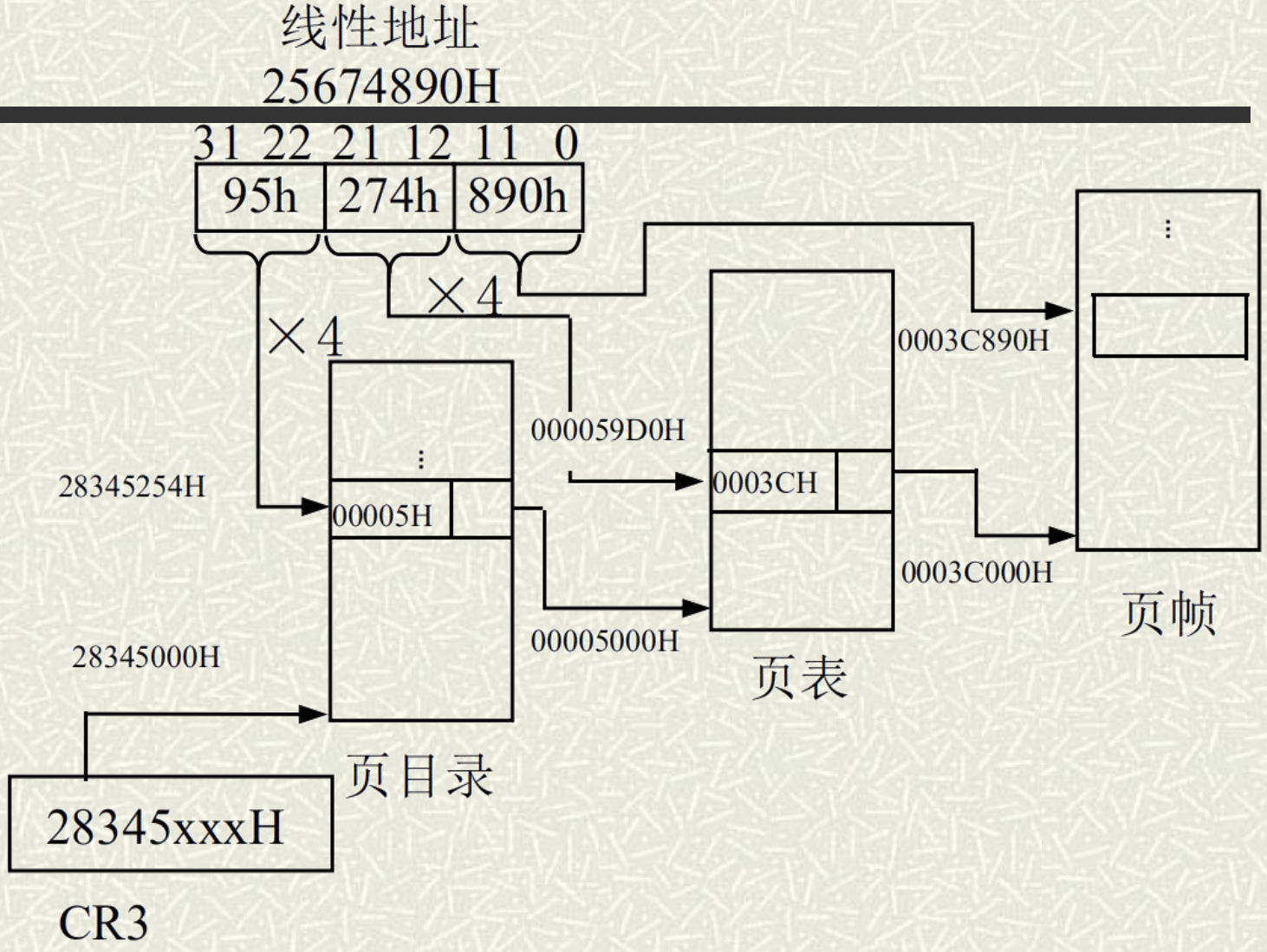


图 5.3 线性地址到物理地址的转换

重点难点例析

解：

1） 将线性地址为25674890H分解为页目录项，页表项及页内偏移量的形式即变为：

31	22	21	12	11	0
0010’0101’01		10‘0111’0100		1000‘1001’0000	
页目录项（10位）		页表项（10位）		偏移量（12位）	

这是通过页目录、页表项及偏移量所进行的正常访问。

重点难点例析

- 2）查询CR3，由于CR3=28345XXXH，所以页目录基地址=28345000H。

- 3）页目录表中所寻址项的物理地址=目录表基地址+偏移地址（目录索引地址╳4）=28345000H+95H╳4=28345254H

重点难点例析

- 4）页表中所寻址项的物理地址=页表基地址+页表索引地址×4
  =00005000H+274H×4=000059D0H

- 其中，页表基地址由页组目录项中高20位所得。

重点难点例析

- 5）要寻址的存储单元最终物理地址=页帧基地址+线性地址中的12位偏移量
  =0003C000H+890H=0003C890H

- 其中，页帧基地址由页表项高20位所得。

返回

Multiple Choice(single) Points: 1

设置

下列几种说法，哪种错。

A 此虚拟存储器是在存储体系层次结构基础上，通过硬件和软件的综合来扩大用户可用存储空间的一种新的计算机存储技术，它提供比物理存储器大得多的逻辑地址空间。

B 无论页式、段式或段页式虚拟存储器都是使用驻留在内存储器中的转换函数表来完成逻辑地址向物理地址变换的。

C 虚拟存储器技术的引入，使CPU可寻址的存储空间范围几乎扩展到无穷大。

提交

作业

- P310
- 2、11、14—写本子上
- 3、4、12、28—问答题可在书上找答案