页表项的基本功能

页表由多个页表项组成，即页表中每一行的就是一个页表项。页表项是操作系统中分页机制的关键组成部分，它实现了虚拟地址空间到物理地址空间的映射。当程序尝试访问内存时，CPU 使用虚拟地址，操作系统通过页表将这个虚拟地址转换为物理地址，从而访问实际的物理内存。

页表项的组成

页表项通常包含以下字段：

一、物理页帧号：

这是页表项中最重要的信息，它指定了虚拟页对应的物理内存页的帧号。物理页帧号实际上是物理地址的页对齐部分，可以与页内偏移结合来形成完整的物理地址。

二、控制位：

1. 存在位（Present Bit）：

也称为有效位，用于指示对应的物理页是否当前在物理内存中。如果存在位为 0，表示该页不在内存中，尝试访问它将导致缺页异常（Page Fault）。

2. 修改位（Dirty Bit）：

用于跟踪页面自从被加载到内存中后是否被写入过。如果页面被修改，修改位将被设置为 1，这样操作系统就知道需要将该页的数据写回磁盘，以确保磁盘上的数据与内存中的数据保持一致。

3. 引用位（Referenced Bit）：

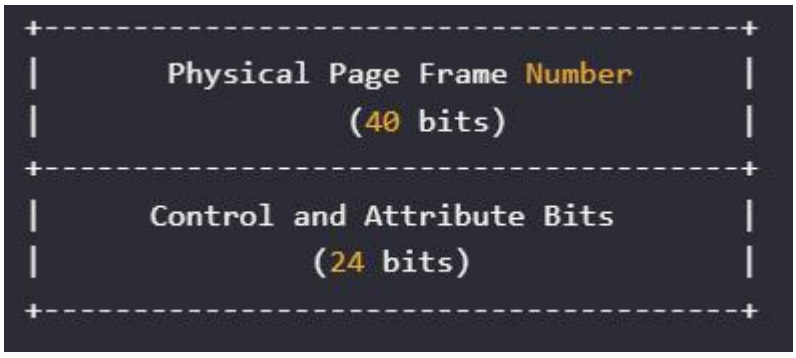
用于指示页面是否在最近被访问过。操作系统可以使用这个信息来进行页面替换算法，优先替换那些未被引用的页面。

4. 权限位（Permission Bits）：

控制对该页的访问权限。通常包括读/写权限，以及是否允许执行该页中的代码。这些权限位有助于操作系统实施安全策略，防止用户程序访问或执行内核空间的代码。

5. 其他控制位：

页表项中的其他控制位用于管理和优化内存访问，包括全局位（Global Bit），用于指示页面是否应该在所有进程的地址空间中保持一致，从而在上下文切换时不需刷新 TLB；缓存控制位（Cache-Control Bits），如缓存禁用位（Cache Disable Bit），用于控制页面数据是否进入 CPU 缓存，以及写合并位（Write Combine Bit），用于直接将数据写入主内存而不进入缓存层次；访问权限扩展位，如用户/系统位（User/Supervisor Bit），用于区分用户空间和内核空间的访问权限，共享位（Share Bit），用于指示页面是否可以被多个进程共享，以及设备位（Device Bit），用于标识页面是否包含设备映射的内存；执行禁止位（No Execute Bit, NX Bit），用于控制页面是否可以执行，从而防止某些类型的攻击；访问标志（Access Flags），包括访问位（Accessed Bit），用于指示页面是否已被访问过，以及修改位（Dirty Bit），用于指示页面是否已被修改过；以及透明大页（Transparent Huge Pages, THP）支持位，用于减少页表项数量并提高性能。这些控制位的组合使用，使得操作系统可以灵活地管理和优化内存访问，同时提供内存保护机制，增强系统的安全性。



x86-64 架构为例，页表项通常是一个 64 位的值，其中包含了物理地址和其他控制位。