

## 作业11 (709A) 表页管理与虚拟内存

### C4 表页管理与虚拟内存

#### 1. 存储器层次与地址映射的实现 (大题)

存储器越快，成本越高；高速存储器件容量小，成本

高，为了综合获得运行速度和成本，采用多层次存储

级，将不同数据存在不同速度和容量的存储器中。

同时不同存储器有带宽限制，有些任务需访问大量数据。

多层次结构可以缩短访问延迟和减轻带宽限制。

综上，达到控制成本，获得尽可能大的存储容量和

读写速度及可靠性的目标。  
由图可知

#### 2.

过大的页：浪费存储空间，页包含的存储容量过大。

程序即使只访问一小部分内存，也要把整页全部加载

到内存中；同时每个进程需要有一定页面，过大的页

会导致进程之间竞争内存资源。

过小的页：需要很多页来存储一个进程，带来更多的

页面表项，使得页表体积变大，且增加内存碎片

化，使得操作系统管理

内存开销变大，内存读写性能降低。

#### 3. 表页向页框映射。指出表页与页框的关系

① V位表明该PTE是否合法，若是0则PTE的31-1bit

位不关心且可以由软件自由使用；

RWX位为权限位，表明该页是否可读、写、执行；

U位表明该页表是否可由U态使用，为1时可由U态使用，

同时若sstatus寄存器中的PUM位清零，则S态软件也可

在U位为1时获取页，但通常其PUM为1，则S态一般不

可以访问用户页；  
由图可知，全局映射的页表项

G位表示全局映射，全局映射是存在于所有地址空间中

的映射，对于非叶PTE，全局映射意味着页面后续级别中

的所有映射表是全局的，不将全局映射在G位中标记只会

降低性能，将非全局映射标记为全局则是错误的；

A获取位，虚拟地址被读写或匹配时，对应PTE的A位

被置位；  
由图可知，全局映射的页表项

D脏位，当虚拟地址被写时，对应PTE的D位被置位。

#### 2) ① 安全性问题

可能会越权访问系统资源和其他进程的内存空间，例

如用户把某些页表标记为内核态。

#### ② 内存管理问题

可能占用或浪费资源，影响其他进程的正常运行，例如用户

把不需要的内存标记为已使用，降低内存利用率。

#### ③ 系统稳定性问题

用户将正在使用的页表指向错误的地址，无法访问正

确的内存空间，导致系统崩溃。



扫描全能王 创建

3) 当 RWX 三者均为 0 时, PTE 是一个指向下级

A=11, 自然对齐的二次幂区域 (NAPOT), 28 字节,

页表的指针; 否则是一个叶页表项

当这位设置被编写时, pmpaddrx 寄存器编低位编

码大小, 上面的位编码基地址右移 2 位, 中间有

一个零位即最低有效零位 (LSZB)。

4. 对于较低的权限等级, PMP 可以授予对设备内有映射的特定区域的权限

5. 64 位虚拟地址  $\rightarrow 2^{64}$  B

1) 对于较低的权限等级, PMP 可以授予对设备内有映射的特定区域的权限

$2^{64} / 4 \times 2^{10} = 2^{52}$  个页表条目

对于 R/W/X 位, 位取 0 时表示对此区域没有读取/写入/执行权限; 位取 1 时表示为此区域授

$2^{52} \times 8 \text{ B} = 2^{55}$  B 空间

予读取/写入/执行权限 (页表条目的区域)

即 32 PB (55 位) 空间

2) L 位: 锁定位

2) 使用 48 位  $\rightarrow 2^{48}$  B

L=0, PMP 进入解锁, 没有权限限制应用到机器模式, PMP 条目仅适用于 S 和 U 模式;

$2^{48} / 4 \times 2^{10} = 2^{36}$  个页表条目

L=1, PMP 的入口被锁定, 对所有权限级别强制执行权限, 对配置和地址寄存器的进一步写入被忽略。

$2^{36} \times 8 \text{ B} = 2^{39}$  B 空间

A 位: 地址匹配模式位

即 512 GB (39 位) 空间

A=00, PMP 入口禁用, 没有对任何权限级别应用

3) 多级页表通过将页表项分散到多个级别的页表中,

A=01, 由两个相邻 pmpaddr 寄存器定义的 TOR 区域,

高级低级页表仅存储高级页表的地址, 第

若 pmocfg 定义 TOR, 则基址是 0x0, pmpaddr 定义上限,

高级页表存储实际的页表项, 则缩小单个页表

只支持四字节粒度;

的大小, 变成原来的平方根级别 (2 级); 且用动态

A=10, 自然对齐的四字节区域 (NA4), 仅支持四字

创建二级表只为实际使用部分分配页面, 均能降低

虚拟内存的实际页表存储开销。

虚拟内存的实际页表存储开销。

通过多次访问的方式节省页表存储空间

→ 时间换空间, 且额外时间开销低

五、PML4E



扫描全能王 创建