

计算机操作系统

自映射

课堂练习

假设一个机器有38位的虚拟地址和32位的物理地址。

- (1) 与一级页表相比，多级页表的主要优点是什么？
- (2) 如果使用二级页表，页面大小为16KB，每个页表项有4个字节。应该为虚拟地址中的第一级和第二级页表域各分配多少位？

课堂练习

3. 假设一个机器有38位的虚拟地址和32位的物理地址。
- (1) 与一级页表相比，多级页表的主要优点是什么？
 - (2) 如果使用二级页表，页面大小为16KB，每个页表项有4个字节。应该为虚拟地址中的第一级和第二级页表域各分配多少位？

答案：

除了顶级页表之外，使得每一个页表都放在一个物理页框中。

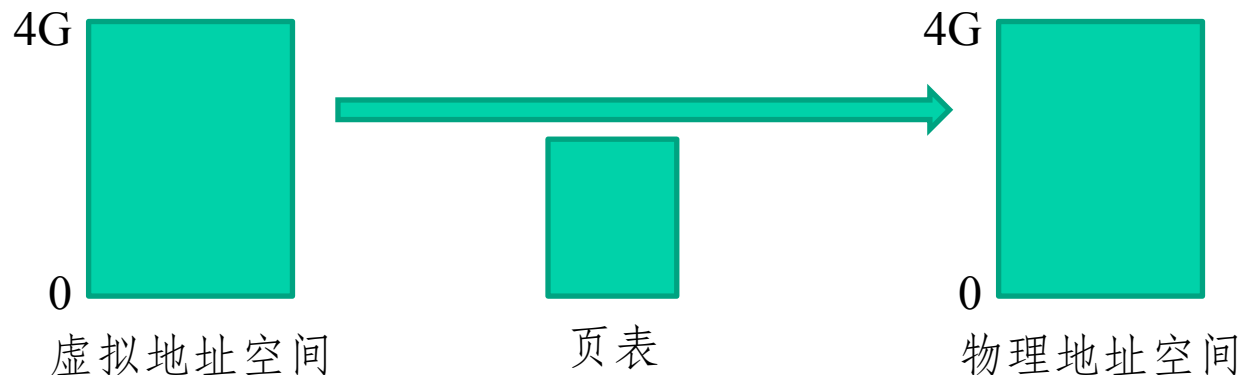
二级页面大小 = $16K/4=4K$ ； 12位。

一级和二级页表域分别需要12位，偏移量需要14位。

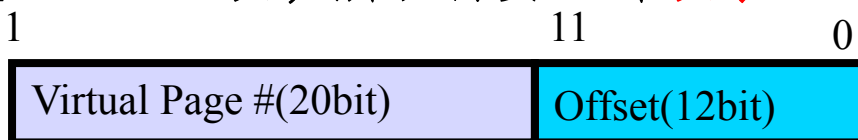
专题：页目录自映射

■ 基本事实：

- 页表的作用是将虚拟地址空间映射到物理地址空间

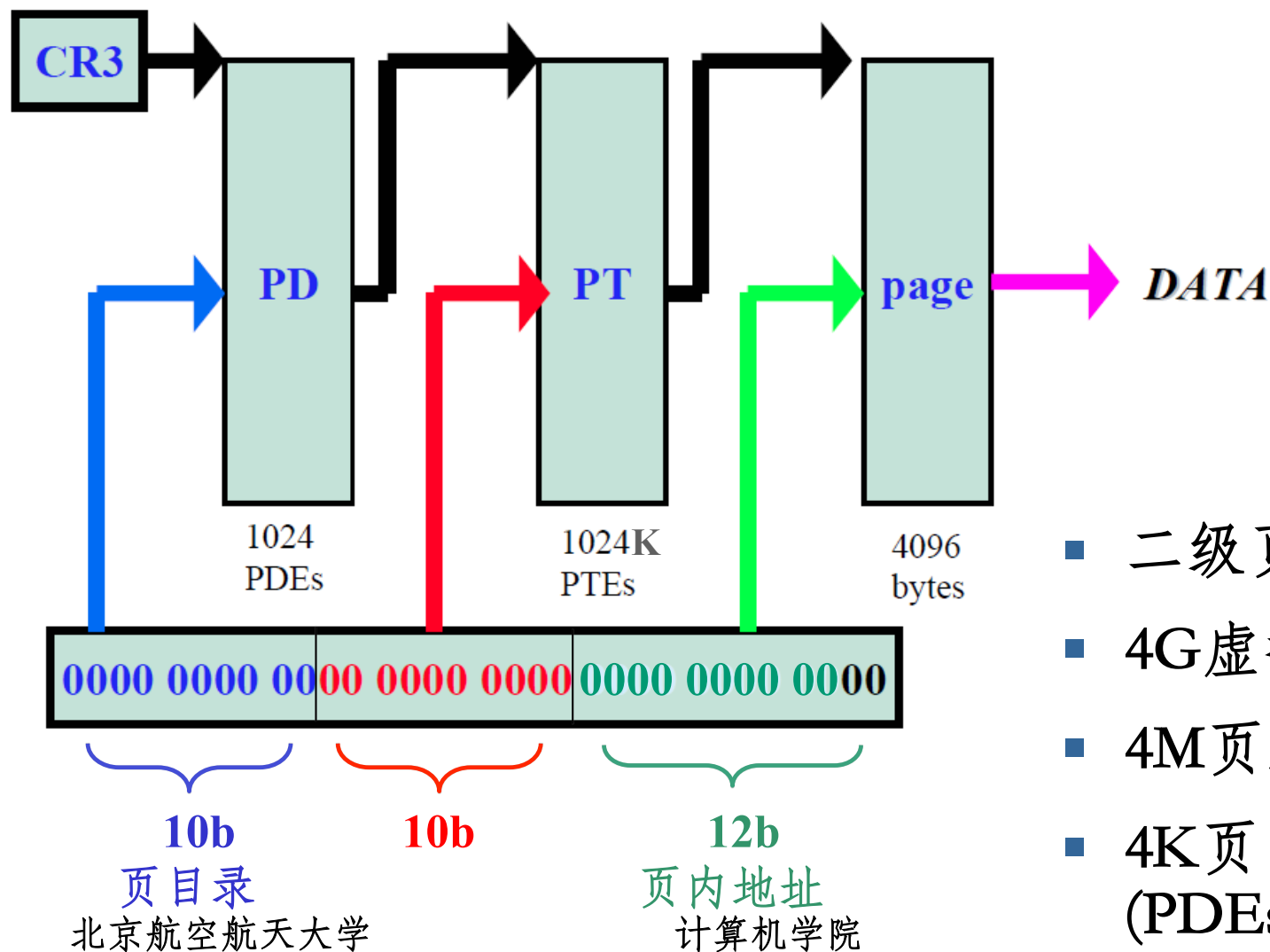


- 对于32位地址长度，可寻址空间为4GB
- 采用12位页内偏移，表明内存页大小为4KB
- 每个页表项负责记录1页（4KB）的地址映射关系
- 整个4GB地址空间被划分为 $4GB/4KB=1M$ 页，所以需要1M个页表项来记录逻辑-物理映射关系



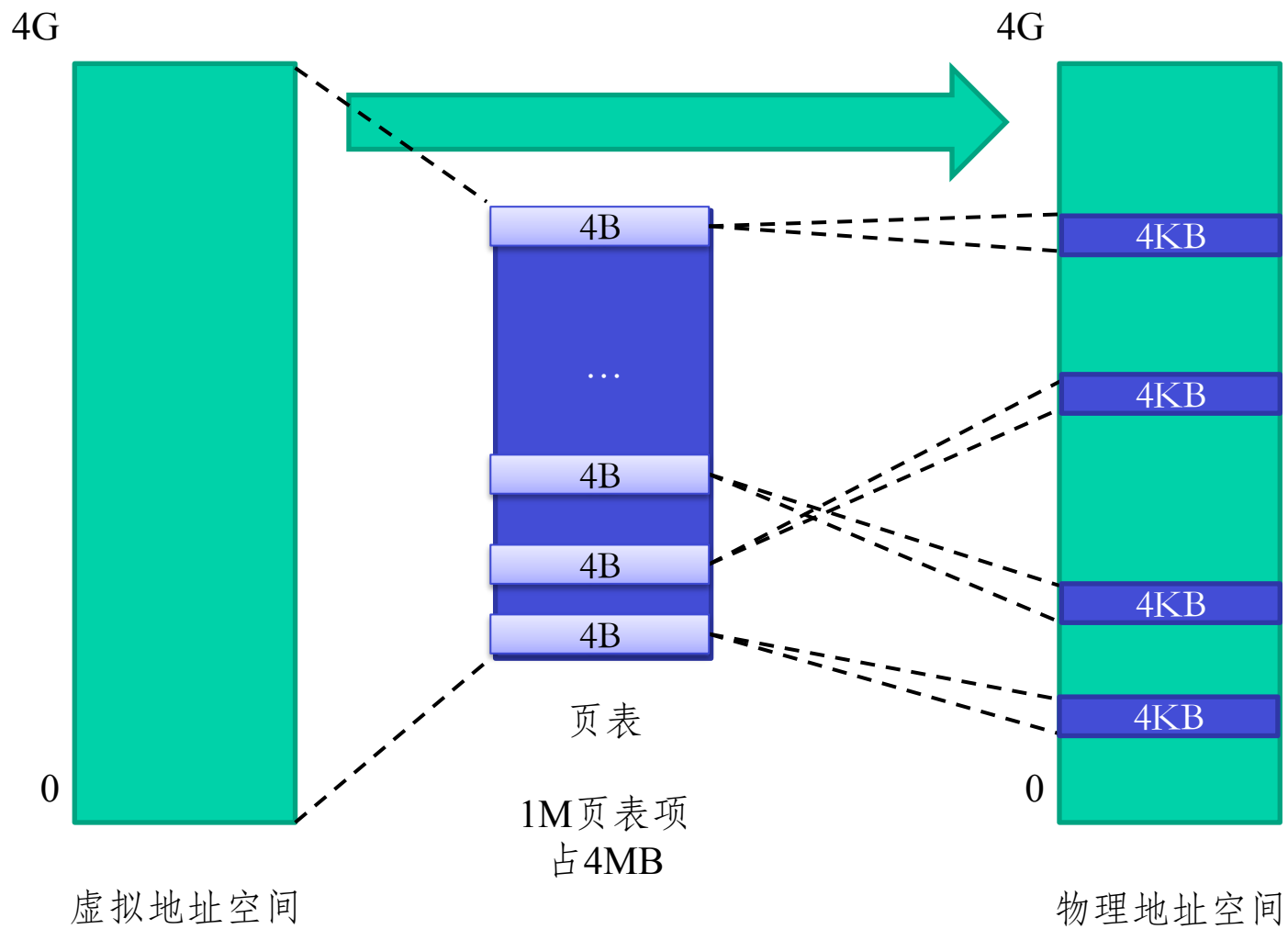
多级页表中，每级页表大小应该正好在一页。一个页表项 4Byte, $4\text{KB}/4\text{B}=1\text{K}=1024$, 所以一级页表10位，剩余二级页表10位，页表合计20位

Virtual Address Translation



- 二级页表
 - 4G虚拟地址空间
 - 4M页表项(PTEs)
 - 4K页目录表项(PDEs)
- 王雷

页目录自映射



页目录自映射

■ 页表也要存储在内存中

- 操作系统对页表访问也通过虚地址
- 页表维护了虚拟地址到物理地址的映射
- 页表也维护了自身虚拟地址到物理地址的映射（自映射）
- 每个页表项需要4字节，所以1M个页表项需要4MB字节存储，所以整个页表占用的内存大小就是4MB

页目录自映射

- 4MB页表也要分页存储，共需要 $4\text{MB}/4\text{KB}=1024$ 页表项
- 所以1M个页表项中，其中有1024个页表项（1个页表）正好描述了页表本身从虚拟地址到物理地址的映射。大小4K。
- X86 二级页表结构中，二级页表=页目录
- 根据二级页表（页目录）的定义：记录页表虚拟地址空间到物理地址空间映射关系的，也就是页目录。大小4K

页目录自映射

- 4MB页表也要分页存储，共需要 $4\text{MB}/4\text{KB}=1024$ 页表项
- 所以1M个页表项中，其中有1024个页表项（1个页表）正好描述了页表本身从虚拟地址到物理地址的映射。大小4K。
- 二级页表结构中，二级页表=页目录
- 根据二级页表（页目录）的定义：记录这4M页表地址空间到物理地址空间映射关系的，就是页目录。大小4K

所以页目录的内容和一个页表（1024页表项）内容一致

页目录自映射

- 4MB页表也要分页存储，共需要 $4\text{MB}/4\text{KB}=1024$ 页表项
- 所以1M个页表项中，其中有1024个页表项（1个页表）正好描述了页表本身从虚拟地址到物理地址

所以页目录的内容和一个页表（1024页表项内容一致）

→ 一个页表和页目录是重合的！

→ 页目录不需要单独映射

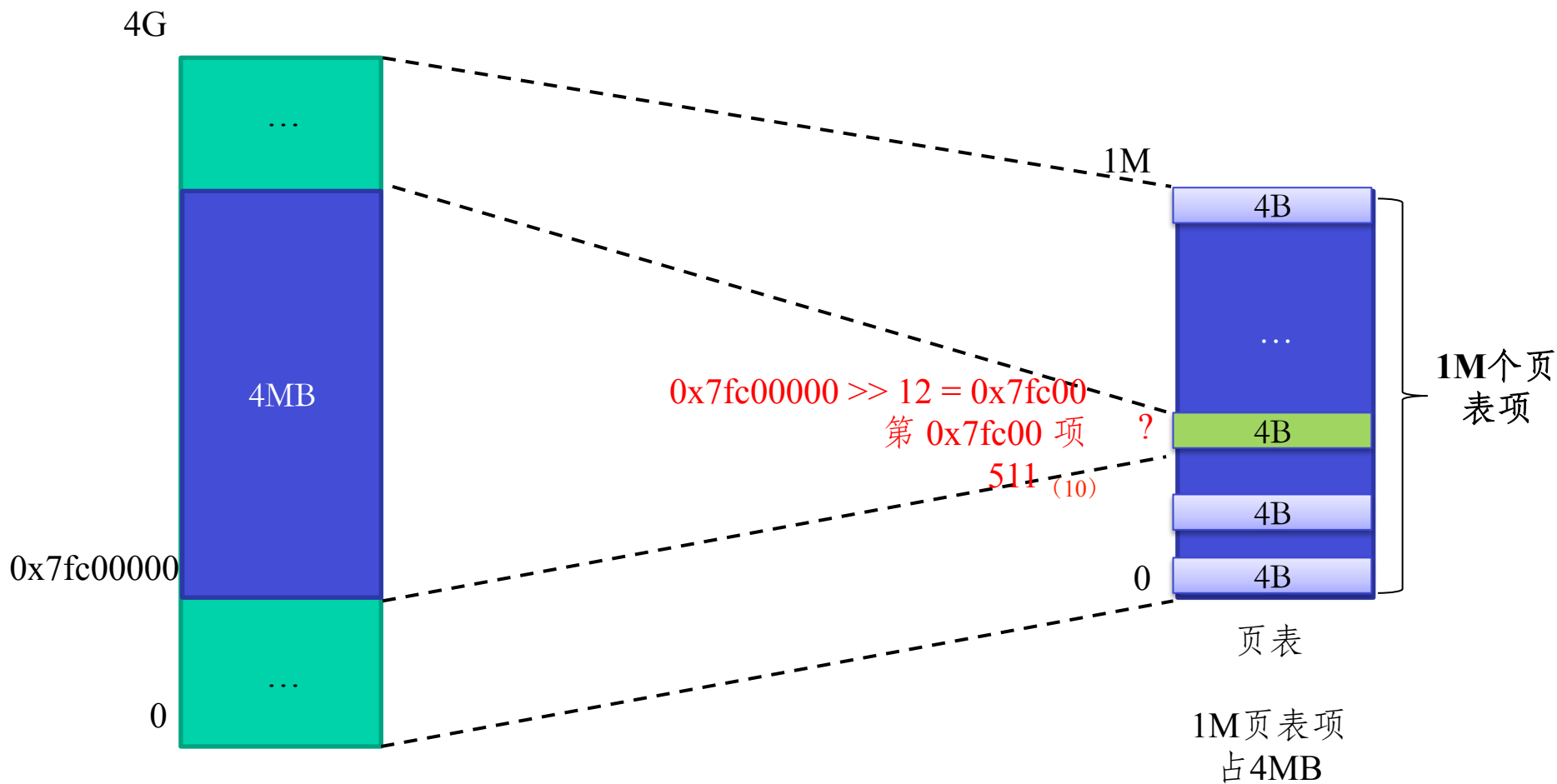
地址空间到物理地址空间的映射关系，就是页目录。大小4K

页目录自映射

■ 页目录在哪？

- 给定页表虚拟地址起始位置，例如0x7fc00000
- 将整个4GB地址空间划分为1MB个4KB页
- 上述地址对应于第 $(0x7fc00000 >> 12)$ 个4KB页，因此其逻辑-物理映射关系应该记录在第 $(0x7fc00000 >> 12)$ 个页表项中
- 每个页表项4个字节，所以该页表项对于的页表起始地址地址偏移为 $(0x7fc00000 >> 12) * 4 = 0x1ff000$

页目录自映射



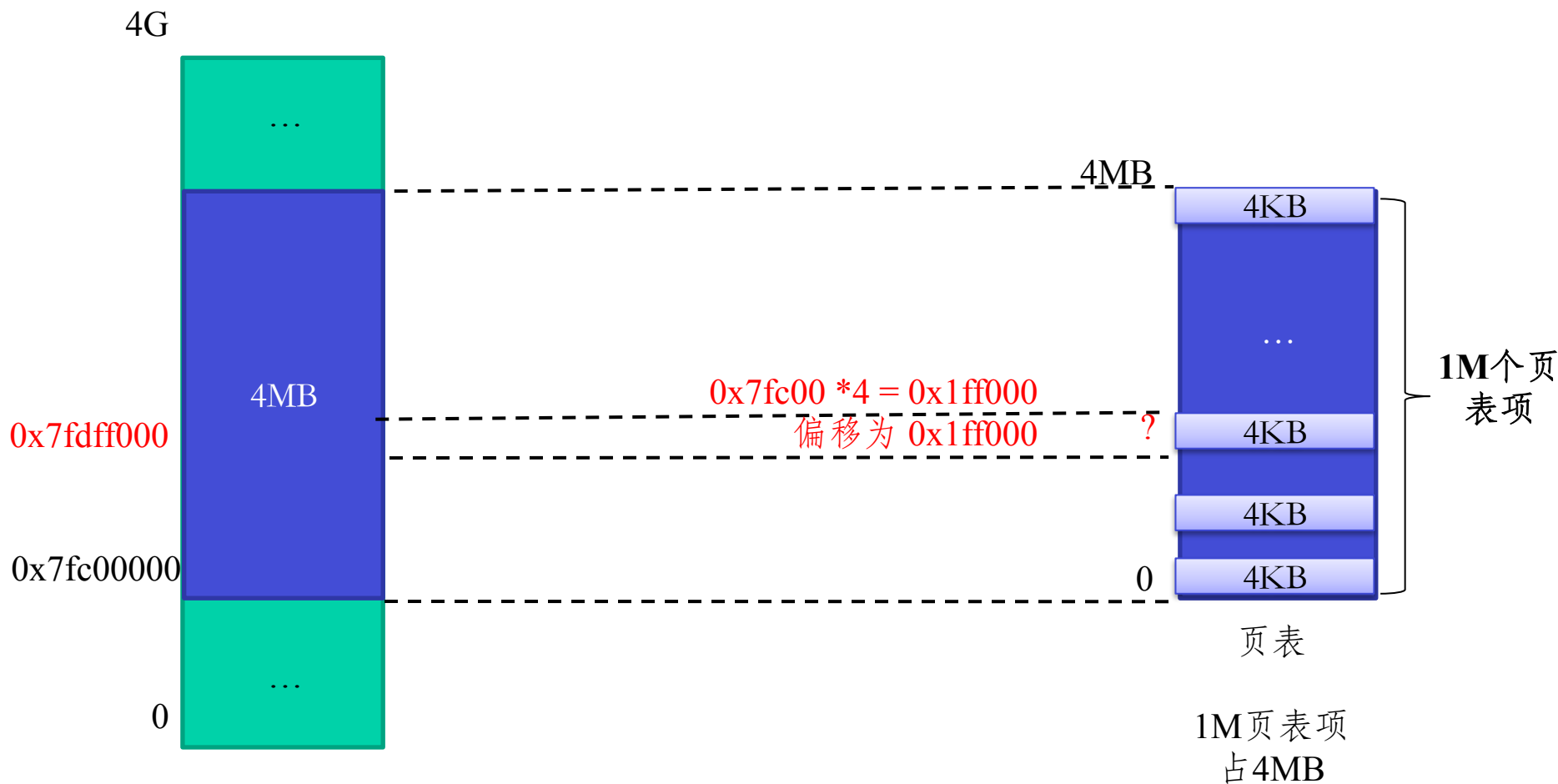
虚拟地址空间

北京航空航天大学

计算机学院

王雷

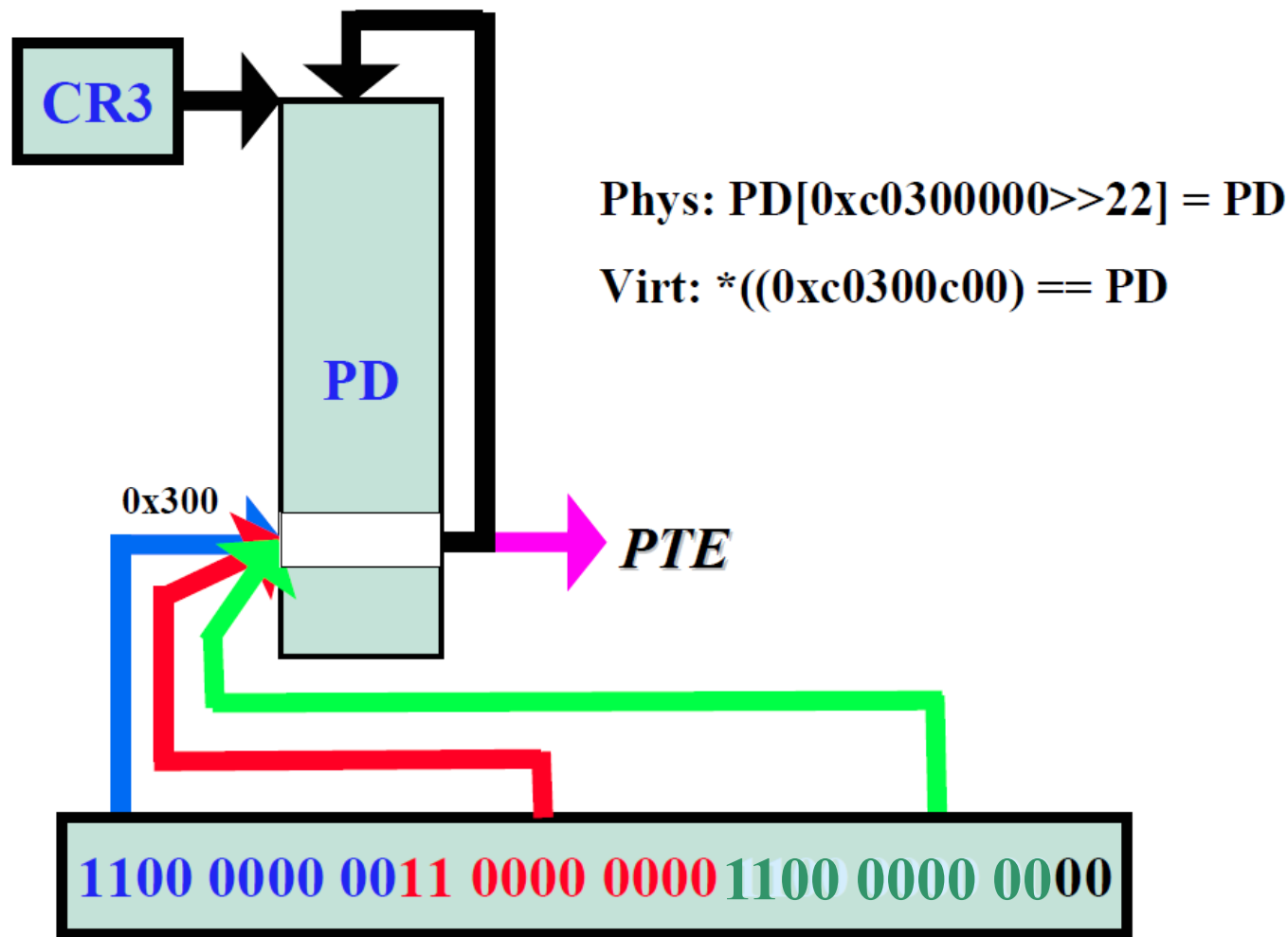
页目录自映射



虚拟地址空间

Win中的页目录自映射

Virtual Access to PageDirectory[0x300]



页目录自映射

■ 简化计算

- 对于32位地址字长，2级页表，4KB页面大小，虚拟地址va
- 页目录PDE地址=：
 - $((\text{PMMPTE})((((\text{ULONG})(\text{va})) \gg 12) \ll 2) + \text{PTE_DASE}))$
- 页表PTE地址=：
 - $((\text{PMMPTE})((((\text{ULONG})(\text{va})) \gg 22) \ll 2) + \text{PDE_DASE}))$

■ 练习：

- 页表起始地址0x80000000，页目录起始地址=？
- $0x80000000 + 0x200000 = 0x80200000$

■ 反过来：如果给定页目录起始地址，求页表起始地址？

- E.g. 页目录起始地址0xC0300000，页表起始？