PA3 实验报告

PA3-2

1. nemu 什么时候进入了保护模式?

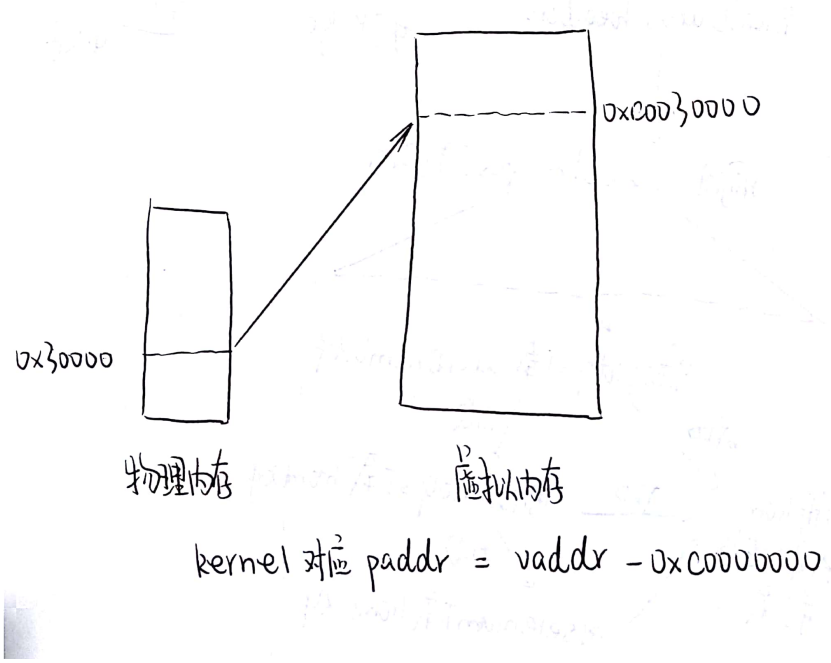
cr0 寄存器中 pe 位被置为 1 之后 nemu 进入了保护模式。

2.gdtr 中保存的段表首地址是虚拟地址？线性地址？还是物理地址？为什么？

保存的是线性地址。因为虚拟地址是通过查段表来转换成线性地址的，然后再通过分页机制转换为物理地址，因此在转换成线性地址过程中用到的段表首地址应为线性地址。

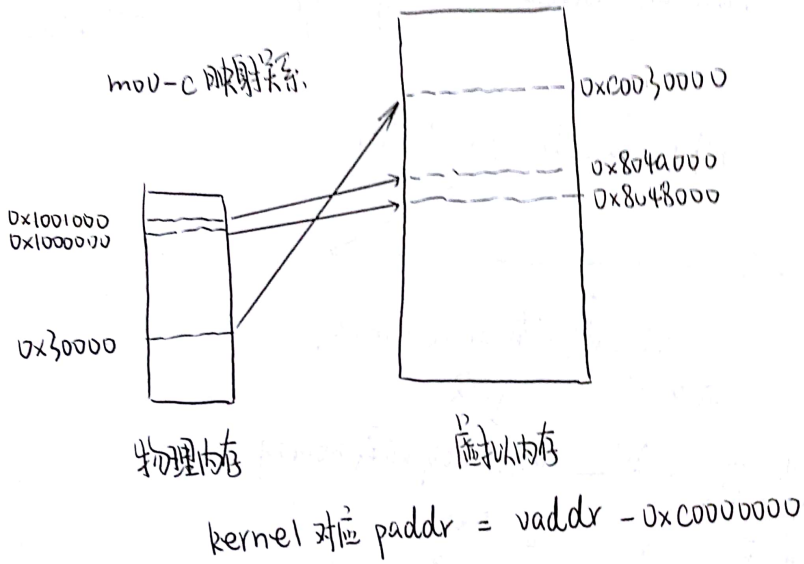
PA3-3

1. Kernel 的虚拟页和物理页的映射关系是什么？请画图说明；



2. 以某个测试样例为例，画图说明用户进程的虚拟页与物理页间映射关系又是怎样的？Kernel 映射为那一段？你可以在 loader()中通过 Log()输出 mm_malloc

的结果来查看映射关系，并结合 init_mm()中的代码绘出内核映射关系。



结合 init_mm()发现 kernel 的映射关系仍然是一样的。

3. “在 Kernel 完成页表初始化前，程序无法访问全局变量”这一表述是否正确？在 init_page()中我们对全局变量做了怎样的处理？

表述正确。因为没有完成页表初始化前，不能通过 ELF 文件中符号表对应的虚拟地址来获得其物理地址，存在虚拟地址到物理地址的映射关系。因此无法访问全局变量。在 init_page()中是通过 va_to_pa 宏将虚拟地址直接减去 0xc0000000 来获得物理地址。