3-2

问题 1：nemu 在什么时候进入了保护模式？

在 lgdt 指令加载好了段描述符表后，CR0 中的 PE 位被置为 1，进入了保护模式。

问题 2：GDTR 中保存的段表首地址的是虚拟地址、线性地址还是物理地址？为什么？

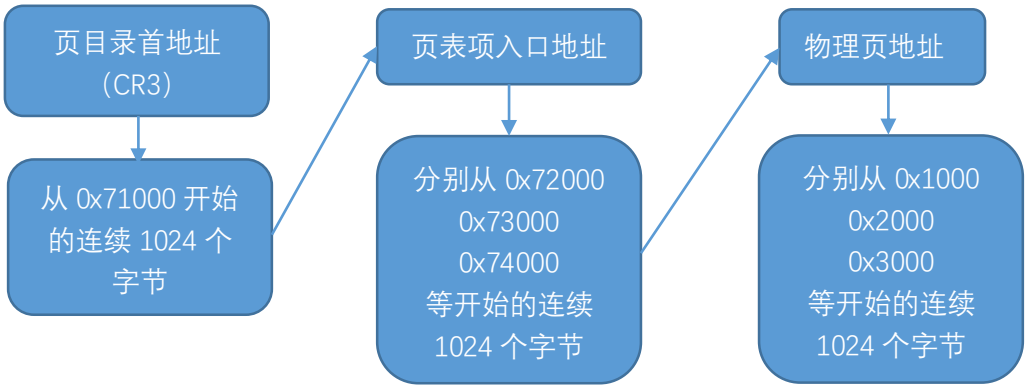
GDTR 中保存的段表首地址是物理地址。

首先因为加载 GDT 时，还没有开启分页机制，因此不存在虚拟地址向线性地址的转换，因此不可能是虚拟地址。

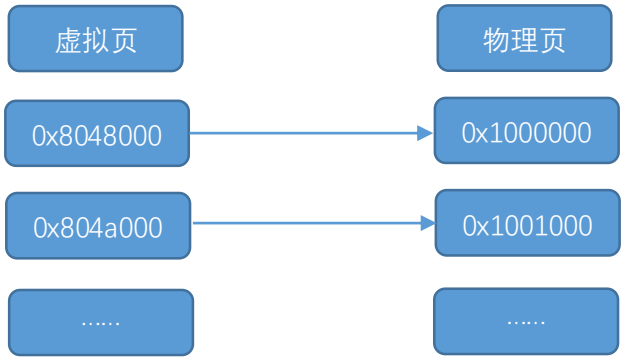
其次，GDT 的功能是负责将线性地址转换为物理地址。如果 GDT 中存放的是线性地址，则该线性地址尚无法转换为线性地址，因此 GDT 中存放的只能是物理地址。

3-3

问题 1：Kernel 的虚拟页和物理页的映射关系是什么?请画图说明;



问题 2：以某一个测试用例为例,画图说明用户进程的虚拟页和物理页间映射关系又是怎样的?Kernel 映射为哪一段?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。



问题 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() 里面我们对全局变量进行了怎样的处理?

这一表述不完全正确，应该说在 Kernel 完成页表初始化前，程序无法通过页表虚拟地址转换来访问全局变量，但是我们可以用其他方式访问到全局变量。在 init_page()函数里，我们 通过 va_to_pa 宏，将虚拟地址-0xc0000000 来进行转换成物理地址，进而访问全局变量。