OS lab11 Report

name: 刘乐奇

sid: 12011327

Ubuntu用户名: lynchrocket

1. 一个进程有多少个mm_struct? mm_struct的作用是什么?

一个进程有一个mm_struct。

每个页表（每个虚拟地址空间）可能包含多个 vma_struct , 也就是多个访问权限可能不同的、不相交的连续地址区间。我们用 mm_struct 结构体把一个页表对应的信息组合起来，包括vma_struct 链表的首指针，对应的页表在内存里的指针， vma_struct 链表的元素个数。

2. vma_struct的作用是什么?

vma_struct 结构体描述了一段连续的虚拟地址，从 vm_start 到 vm_end 。 通过包含一个 list_entry_t 成员，我们可以把同一个页表对应的多个 vma_struct 结构体串成一个链表，在链表里把它们按照区间的起始点进行排序。它的成员 vm_flags 表示的是一段虚拟地址对应的权限（可读，可写，可执行等），这个权限在页表项里也要进行对应的设置。

3. 什么情况下会出触发缺页中断?

当cpu访问虚拟地址，而该虚拟地址找不到对应的物理内存时触发该异常。

1. 页表中没有虚拟地址对应的PTE（虚拟地址无效或虚拟地址有效但没有分配物理内存页）
2. 现有权限无法操作对应的PTE

4. major page fault是如何处理的？在实验代码中对应哪一段?

major page fault 即访问的虚拟地址内容不在内存中，需要从外设载入。常见于内容页被置换到外设交换区中，需要将交换区中的页面重新载入内存。

在实验代码中，CPU 抛出 page fault 的时候，kern/trap/trap.c 的 exception_handler() 会处理相关的异常，并最终交由 do_pgfault() 这个函数进行处理。 该函数在 kern/mm/vmm.c 中。