操作系统Lab5 实验报告

2012011350 计24 周琳钧

练习0：填写已有实验

1. 实验过程：主要是四个地方需要添加一些代码。一个是中断门设置时要将0x80这个中断向量赋为用户态，其实这个在我Lab1的代码中已经做出了更改，第二个是时钟到达100时无需输出100 ticks，要变成设置当前线程的need\_resch为1，表示它需要重新部署，第三个是分配进程初始化时多出了wait\_state, cptr, yptr, optr这几个变量均要初始化，第四个是do\_fork函数中可以使用新构造的函数set\_links()将新进程接入进程链表中。

练习1：加载应用程序并执行

1. 实验过程：我们需要补充proc.c中loadicode中函数，整个用户进程产生过程将在稍后的问答题中说明。本练习需要补充用户进程环境的中断帧，即将硬盘中内容调入虚拟内存的最后一步。实验步骤十分简单，只需按要求设置tf\_cs为USER\_CS，tf\_ds, tf\_es, tf\_ss为USER\_DS，tf\_esp指向栈顶，tf\_eip指向程序入口地址，tf\_eflags设置成FL\_IF即可。
2. 问答题：首先操作系统先创建了内核线程idle\_proc，然后由其创建了第二个内核线程init\_proc，然后继续创建了第三个进程——用户进程，创建方法是调用user\_main函数，然后调用KERNEL\_EXECVE宏，在输出一些调试信息后调用kernel\_execve函数，执行系统调用，然后该进程进入等待模式，一旦时间片被分给了用户进程，执行proc\_run切换到该用户进程并执行相应语句。

练习2：父进程复制自己的内存空间给子进程

1. 实验过程：本实验要完成父进程的资源向向子进程的写入过程。假设我们知道了父进程的start地址，end地址和一级页表地址和子进程一级页表地址。我们的做法是：循环拷贝父进程的每一页至子进程，具体做法是通过页表找到该页，并将其转化为虚拟地址，执行拷贝过程，若子进程页不存在则分配一个新页，并将其与物理地址相对应即可。
2. 问答题：在dup\_mmap函数中先不必调用copy\_range函数，取而代之的是将父进程资源起始地址赋给子进程，然后当子进程执行过程中资源发生了改动，再调用copy\_range函数为其分配空间。

练习3：弄懂进程的复制，执行，等待，退出的状态转换

1. fork函数会创建一个子进程，并将其赋为PROC\_RUNNABLE，exec函数当进程数为0时会释放掉所有空间，否则为当前进程分配空间，但并不会涉及到状态的转换，wait函数当发现进程为PROC\_ZOMBIE时会将其kill掉，否则会将其赋为PROC\_SLEEPING，exit函数当发现进程标识为PF\_EXISTING时会将其kill掉，否则调用wake\_up函数将其赋为PROC\_RUNNABLE.

exit

wakeup

wait

schedule

fork

Running

Ready

Exit

Block

New