

## Lab3 实验报告

141242026

刘驭壬

邮箱: 141242026@smail.nju.edu.cn

### 实验进度

1. 我将 Lab2 中未完成的分配用户栈切换特权级部分完成。
2. 我完成了 lab3 中要求的所有部分。
  - 1). 实现了 ENV 结构体
  - 2). 实现了各个进程管理函数在(env.c 中)
  - 3). 实现了 ENV 回收机制
  - 4). 实现了 fork,sleep,exit 系统调用 (采用时间片轮转法调度)。

### 关于实验的说明

1. 在本次实验中, 所有的 PCB 均用 ENV 表示 (按照 JOS 框架)
2. 实现了进程的回收机制 (env\_free 函数)。

```
void env_free(struct Env* e){
    pte_t *pt;
    uint32_t pdeno,pteno;
    physaddr_t pa;
    if(e==curenv)
        lcr3(PADDR(entry_pgdir));|
    for(pdeno=0;pdeno<PDX(UTOP);pdeno++){
        if(!((e->env_pgdir[pdeno]&PTE_P)|| (entry_pgdir[pdeno]&PTE_P))
            continue;
        pa=PTE_ADDR(e->env_pgdir[pdeno]);
        pt=(pte_t*)KADDR(pa);
        for(pteno=0;pteno<=PTX(~0);pteno++){
            if(pt[pteno]&PTE_P)
                page_remove(e->env_pgdir,PGADDR(pdeno,pteno,0));

        }
        e->env_pgdir[pdeno]=0;
        page_decref(pa2page(pa));
    }
    pa=PADDR(e->env_pgdir);
    e->env_pgdir=0;
    page_decref(pa2page(pa));

    e->env_status=ENV_FREE;
    e->env_link=env_free_list;
    env_free_list=e;
}
```

释放进程页表并将进程放回 env\_free\_list

3. 对于三个系统调用的实现对错的测试, 我在 game.c 中分别写了 test\_fork(),test\_sleep(),test\_exit(),只要在 Makefile 中修改 game 的入口就行。

```
$(GAME): $(GAME_O) $(LIB_O)
#echo $(GAME_O)
#ehco "*****"
$(LD) -m elf_i386 -e exit_test -nostdlib -o $@ $^ $(shell $(CC) $(CFLAGS) -print-libgcc-file-name)
```

### 我遇到的问题

1. 在 init\_segment 中用到了这个 gdt 数组。我一开始没有加 static, 后来进入 game 的时候一直无法进行中断相应 (缺页)。后加上 static 后可以运行。原因是识别到

了 boot 里定义的 gdt

```
/* GDT in the kernel's memc
static SegDesc gdt[10];
```

2.下面那里要添加 if 语句，防止 do\_timer 为空

```
else if (tf->irq == 1000) {
    //printk("time\n");
    if(do_timer)
        do_timer();
}
```

原因是如果没有加 if 语句，当刚进入 game\_main 的时候还没执行指令，第一个时间中断到来，此时由于 do\_timer 函数指针为空（因为 set\_time\_handler 在 init\_game 中执行，还没执行的时候 do\_timer 指针未被赋值），所以执行的时候会发​​生缺页。