PA4 实验报告

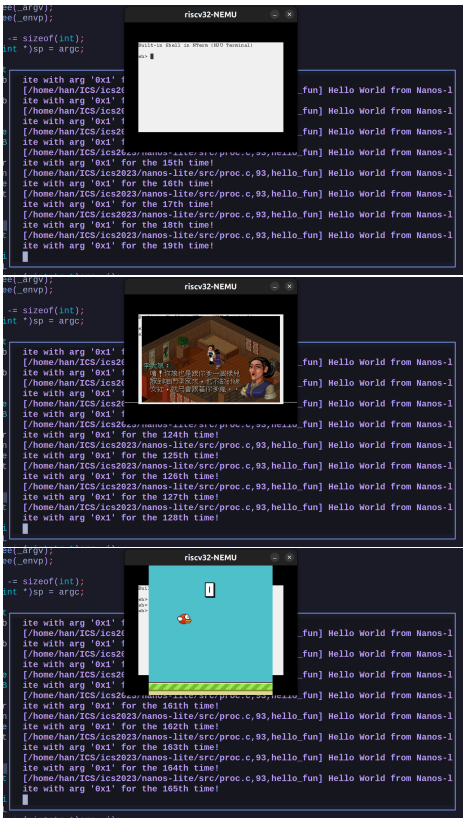
韩加瑞

2024 年 1 月 12 日

1 实验进度

已完成：所有必做内容

完成情况展示：



说明：nanos-lite 初始化完成后默认打开 nterm 程序，在 nterm 里面输入程序名如 pal、bird 等可以打开该程序，按下 0 或 1 切换页面，0 切换到 nterm 界面，1 切换到打开的程序界面，最多只能打开一个程序，之前的程序会被覆盖。此外 nanos-lite 默认后台运行内核程序 hello-fun，频率为每秒运行两次，参数为 1。

2 必做题

2.1 分时多任务的具体过程

分页机制确保了仙剑奇侠传和 hello 程序运行时互不影响，硬件中断确保两个程序按时切换，分时运行。

首先是分页机制在 nanos-lite 中为两个用户程序分别分配用户空间和用户栈，在加载程序时将两个程序加载到不同的地址，并分别维护一份页目录和页表，记录虚拟地址对应的物理地址。之后程序运行时 NEMU 可以根据当前对应的页目录和页表，将虚拟地址转换为物理地址，从而正确的存取数据，不会访问或修改其他用户程序的空间和数据。这样两个程序运行时不会相互影响。

之后是硬件中断按照 60hz 的频率发起时钟中断，从而调度程序可以根据当前程序的运行时间来决定是否切换到另一个程序，这可以通过上下文切换完成。用户程序的上下文（例如指令地址、页目录地址、GPR 等信息）保存在内核空间中。在切换到当前程序前，AM 会将保存在上下文中的信息装载到 nemu 中的 GPR、CSR、PC 中，恢复程序之前的状态，使其能够正确运行。从而通过硬件中断就可以按时切换两个程序，让其分时运行。

2.2 理解计算机系统

编译器会将字符串”abc” 保存在只读数据区，并将 p 为该字符串的首地址。链接器则将该字符串链接到只读数据段。操作系统在将该程序加载到内存中时会将保存只读数据段的页面权限设置为不可写。在执行

```
p[0] = 'A'
```

这条指令时，硬件首先会读取 p 的值，并在页表中检索该地址指向的页面。由于该地址指向的页面不可写，因此发生访问越权的异常，硬件会跳转到

操作系统的异常处理程序入口并执行对应的异常处理程序，向该进程发送 SIGSEGV 信号，并调用内核函数 abort 来终止当前进程，显示段错误。