Lab 实验报告 V

Lab: Lazy Allocation

丁睿

dromniscience@gmail.com

更新：2020 年 11 月 29 日

目录

1 任务完成清单

Subtask	Done?	Time
Eliminate allocation from `sbrk()`	Y	15min
Lazy allocation	Y	30min
Lazytests and Usertests	Y	1.5h

Grade: 119/119

2 详细情况 & 困难和收获

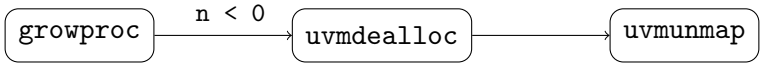
我的作业已开放在这个网页上。

由于暂时未将 Lazy allocation 的策略和之前实现的进程级用户页表结合起来，本次 lab 工作量不大。

实现了 lazy allocation 过后，最大的问题在于用户的虚存空间不再连续。当然，代码、数据、用户栈还是连续的，只是由于现在必须访问堆空间才会分配相应的页，可能出现不连续的情况[1]。于是，代码中使用了连续性假定进行用户空间维护的一切函数必须修改使得符合现在的情形。实际上，这正是本次 lab 后两个阶段的主要工作。

2.1 Eliminate allocation from `sbrk()`

注意 `sbrk()` 既可以扩大堆空间也可以收缩堆空间。当扩大堆空间时，应当增加 PCB 中的 sz 项的大小。而当收缩堆空间时，就应当使用 `growproc()` 释放空间。注意以下调用链:



`uvmunmap` 默认是按照连续的区间进行访问的。为此，我们要修改这两种情况为 `continue;` 即:

```
1 if((pte = walk(pagetable, a, 0)) == 0) continue;
2 if((*pte & PTE_V) == 0) continue;
```

2.2 Lazy allocation

我们要在 `usertrap()` 中增加对缺页的处理。这可由如下条件判断:

[1] 另一种设计是 `sbrk()` 分配比当前访问地址低的所有用户空间的页，但这样显然违背了 lazy allocation 的初衷。因此 `sbrk()` 必须一次仅分配至多一页

```
if(r_scause() == 0xD || r_scause() == 0xF)
// 0xD load page fault
// 0xF store page fault
```

由于 page fault 只能发生在堆段，因此需要检查地址是否合法。下界由 `p->trapframe->sp`(栈顶) 给出，上界由 `p->sz` 给出。如果新的用户页分配失败或者将物理地址注册到用户页表的 `mappages()` 函数失败，则将标记 `p->killed` 以强制结束当前进程并释放资源。

应当注意，另一种需要手动分配未分配页的场景是`sys_read()`或者`sys_write()`，它们在内核级下当即读写一个未分配的地址，因此无法使用缺页处理向量。通过追踪，我们的注意归结到了 kernel/vm.c 文件中的`walkaddr()`函数中。只要我们效仿刚才却也处理程序的处理就可以进行。

注 同样需要在`walkaddr()`中判断地址的合法性。usertests 中的 copyin 特别测试了这一点。它故意写一个高地址的页。

2.3 Lazytests and Usertests

值得庆幸的是，在我做到这个 phase 之前，就已经完成了其中大部分的工作。因此这个阶段完成得较快。

除了上面的几点内容，还有如下的函数需要修改:

`usercopy()` `fork()` 使用该函数复制父进程的用户虚存的内容。默认虚存空间是连续的，因此我们也要将相关判断 (前文代码列出的那两条) 的处理方式从 `panic()` 改为 continue。

`walkaddr()` 紧接着读写一个 `sbrk()` 的地址时调用此函数将报错。应当注释掉其中关于`pte == 0`和`PTE_V`的检查，用上文提到的缺页处理函数替代它。因为该缺页不能被用户态进入内核态的 trap 处理向量捕获，必须单独地实现分配物理页并在用户页表里注册该表项的细节。

3 参考资料

1. *xv6: a simple, Unix-like teaching operating system*
   Russ Cox, Frans Kaashoek, Robert Morris *August 31, 2020*
2. *The RISC-V Reader: An Open Architecture Atlas*
   David Patterson, Andrew Waterman *1st Edition*
3. 现代操作系统 [M]
   A.S.Tanenbaum, H. Bos 著, 陈向群 马洪兵 译, 北京: 机械工业出版社, 2011: 47-95