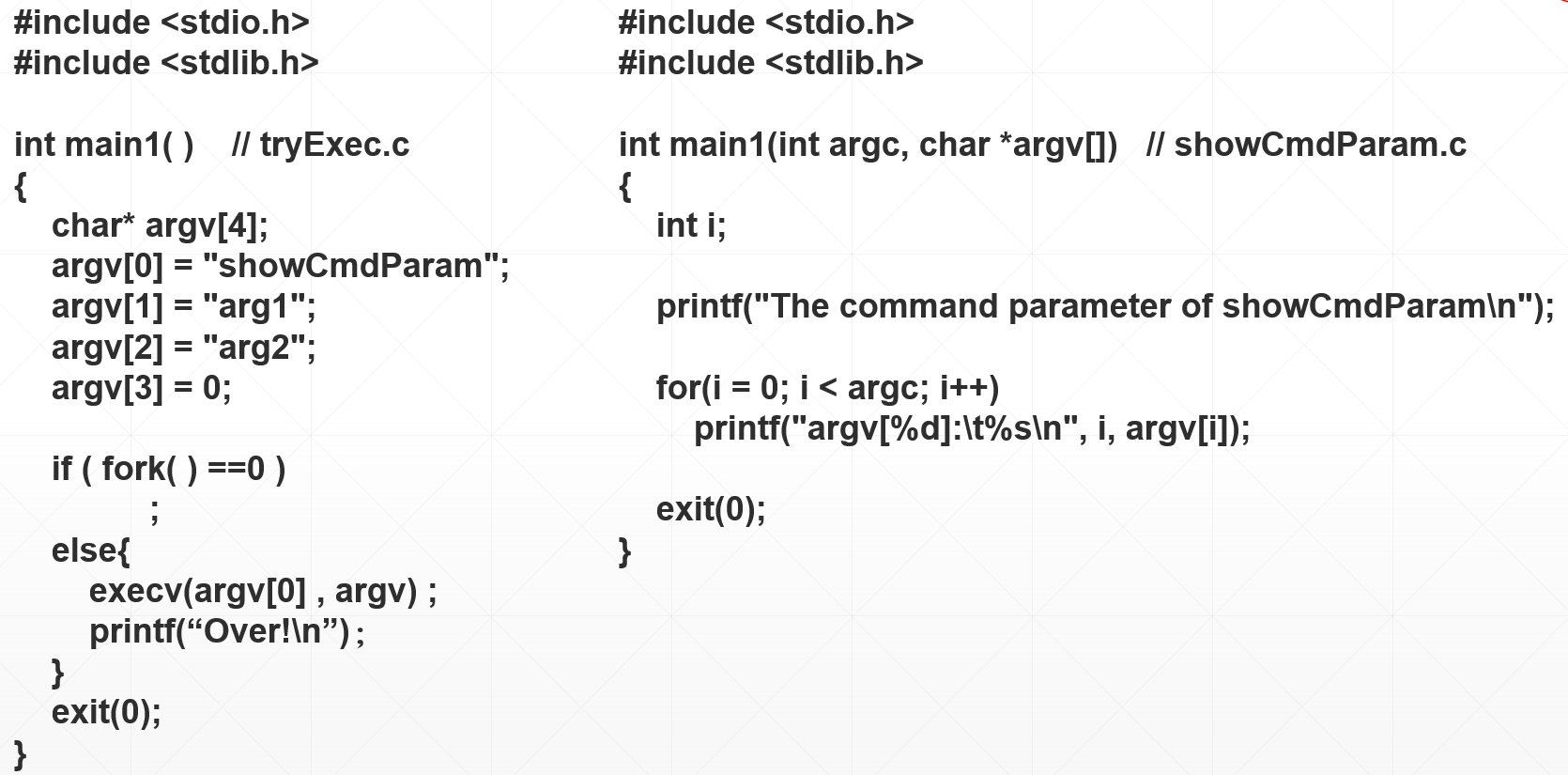
**exec 和 堆空间管理**

同济大学计算机系 操作系统作业 2023-12-7

学号 2151769 姓名 吕博文

1. 这个程序的输出是什么？



**程序输出：**

The command parameter of showCmdParam

argv[0]:showCmdParam

argv[1]:arg1

argv[2]:arg2

注意（1）输出没有“over！” 因为，execv不是普通的子程序调用，装载新程序showCmdParam后，原先用户空间中的tryExec程序没了，进程执行不到printf(“Over!\n”)这条语句。（2）本题，是父进程在转换进程图像

二、现运行进程 PA，1页代码，1页数据，没有只读数据 和 bss，1页堆栈。代码段起始 0x401000。进程依次执行下列动态内存分配释放操作。

char \*p1= malloc(4) ;

char \*p2= malloc(4) ;

char \*p3= malloc(32) ;

free(p2);

char \*p4= malloc(8) ;

free(p1);

char \*p5= malloc(8) ;

1. 指针 p1 的值是多少 ？

首先，进程首次执行malloc，在数据段首端执行brk系统调用分配三个页的大小，并在开头0x403000分配一个flist哑元，之后p1申请4字节空间，加上flist大小为8字节一共12个字节，实行8字节对齐，所以紧接着malloc\_begin之后分配一段长度为16字节的空间，p1 = 0x403010.

1. 指针 p2 的值是多少 ？

P2申请4字节空间，加上flist的大小一共12字节，实行8字节对齐，一共16字节，在空闲区中寻找到第一个大于等于16字节的空间，分配给p2 = 0x403020.

1. 指针 p3 的值是多少 ？

P3申请32字节的空间，加上flist大小一共40字节，在空闲区中寻找到这样一段空间，分配给p3 = 0x403030.

1. 指针 p4 的值是多少 ？

Free(p2)操作之后，p1的nlink直接指向p3，在所有空闲区中寻找16字节的空间时直接找到了上次p2被释放的空间，于是p4占有原来P2的空间，p4 = 0x403020.

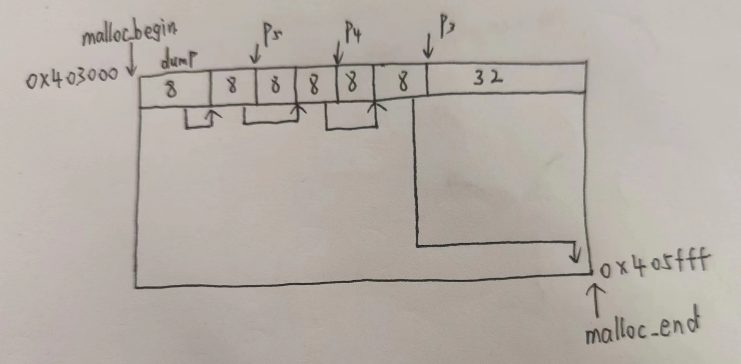
1. 指针 p5 的值是多少 ？

Free(p1)之后，malloc\_begin的nlink直接指向p4，在所有的空闲区中寻找长度为16字节的空间时，直接找到了上次被释放的p1的空间，于是p5占有p1的空间，p5 = 0x403010.

1. 情景分析

上述求得指针值的过程即为具体的情景分析

(7) 画最终的堆结构图



p1 = 0x403010（内存片浪费4字节）

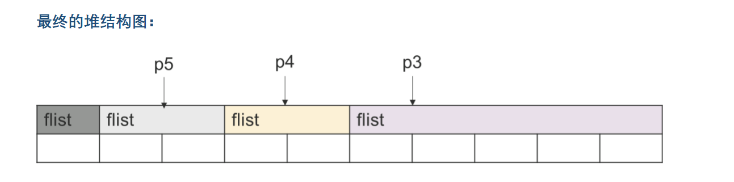
p2 = 0x403020（内存片浪费4字节）

p3= 0x403030

p4 = 0x403020（p2释放的内存片刚好够用）

p5 = 0x403010（同上）

p5执行malloc，发现哑元和分配给p4的内存片之间的空闲区（16字节）刚好够用，用该空闲区装新内存片（没有浪费空间），返回地址是0x403010。



1. 简述tryExec进程创建子进程的过程

tryExec进程执行fork 2号系统调用，为子进程分配空闲的process项，调用Newproc()过程创建子进程，将父进程图像完整复制到子进程图像中，之后父进程返回新创建的子进程的pid号，子进程返回0.

1. 简述程序showCmdParam的加载过程

TryExec进程执行execv 11号系统调用，首先系统调用入口函数分析命令行参数个数和具体内容传给Exec函数，Exec函数寻找可执行文件并确定其运行权限，初始化工作完成之后重构进程图像包括text结构，数据段，堆栈段等等，系统调用返回用户态之后，之心runtime函数驱动应用程序，新的进程从main函数的第一条指令开始执行showCmdParam进程

五、简述子进程showCmdParam进程的终止过程

子进程showCmdParam进程正常执行完毕以后，执行eixt(0)系统调用，由父进程执行wiat系统调用回收子进程的PCB，返回终止码，进程结束。

二、三、四，不必过于详细。要求掌握相关PPT的标题和主干步骤。