**make debug**

增加了

TERMINAL :=gnome-terminal  
debug: targets  
$(V)$(QEMU) -S -s -parallel stdio $(QEMUOPTS) -serial null &  
$(V)sleep 2  
$(V)$(TERMINAL) -e "cgdb -q -x tools/gdbinit"

但还是无法单步执行，求教

[lab2](mhtml:file://Z:\liunix\doc\make%20debug.mht!https://piazza.com/class/i5j09fnsl7k5x0?cid=161)

Attachments:

the instructors' answer,

where instructors collectively construct a single answer

如果能连接上你的机器，也许更好地解决这样的问题。

或者用实验楼  <http://www.shiyanlou.com/>   注册个账号，告诉助教或老师，老师用你的账号去看你的实现？看看能否重现你的问题？

我也不会单步调试，将qemu与gdb连接后设置了断点，输入c执行，结果qemu那边直接跑完了，不会停下来，在lab1时同样的办法qemu会停下来可以单步执行。

qemu

qemu -S -s -hda ucore.img -parallel stdio

gdb

target remote:1234

file ./bin/kernel

b kern\_init

c

输入c后qemu就直接跑完了。

引自qq群小鱼的回答，这里对他表示感谢

“由于lab2，在kern\_init的时候，分页机制还没有建立起来，而符号表中的地址是逻辑地址，所以断点kern\_init不可达，将gdbinit中  break kern\_initg改成 break \*0x0010002a   将断点直接设置物理地址     可以根据符号表文件中逻辑地址0xc010002a得出物理地址 ”

QQ图片20150405203256

不过这种调试有些不直白，也欢迎其他同学提出调试的好方法

但是这样设置断点后没办法调试，输入n后会卡住。

(gdb) b \* 0x001040bf

Breakpoint 1 at 0x1040bf

(gdb) c

Continuing.

Program received signal SIGTRAP, Trace/breakpoint trap.

pmm\_init () at kern/mm/pmm.c:286

286 pmm\_init(void) {

(gdb) n

（这里卡住没有响应，接着输入 ctrl + c）

Remote communication error. Target disconnected.: Connection reset by peer.

/build/buildd/gdb-7.7/gdb/target.c:3293: internal-error: Can't determine the current address space of thread process 42000

请问这个地址是哪个函数的？我这里使用n是可以继续单步执行的

pmm\_init()

换成kern\_init()也不行

仍然卡住么？可以这样尝试。首先

make clean

然后将memlayout.h中的

#define KERNBASE            0xC0000000

改成

#define KERNBASE            0x00000000

修改Makefile中的

$(UCOREIMG): $(kernel) $(bootblock) $(kernel\_nopage)

$(V)dd if=/dev/zero of=$@ count=10000

$(V)dd if=$(bootblock) of=$@ conv=notrunc

$(V)dd if=$(kernel) of=$@ seek=1 conv=notrunc

为

$(UCOREIMG): $(kernel) $(bootblock) $(kernel\_nopage)

$(V)dd if=/dev/zero of=$@ count=10000

$(V)dd if=$(bootblock) of=$@ conv=notrunc

$(V)dd if=$(kernel\_nopage) of=$@ seek=1 conv=notrunc

修改tools/gdbinit中的

file bin/kernel

为

file bin/kernel\_nopage

最后就可以进行调试了

make debug

make gdb

这次可行了，谢谢。

f