6.S081 : Q&A

Approach : staff solutions
start w. pgtbl

Pgtbl lab

- few lines of code, but hard-to-debug problems
- harsh environment
- hard for staff

historically been hard
hardest labs

page tables

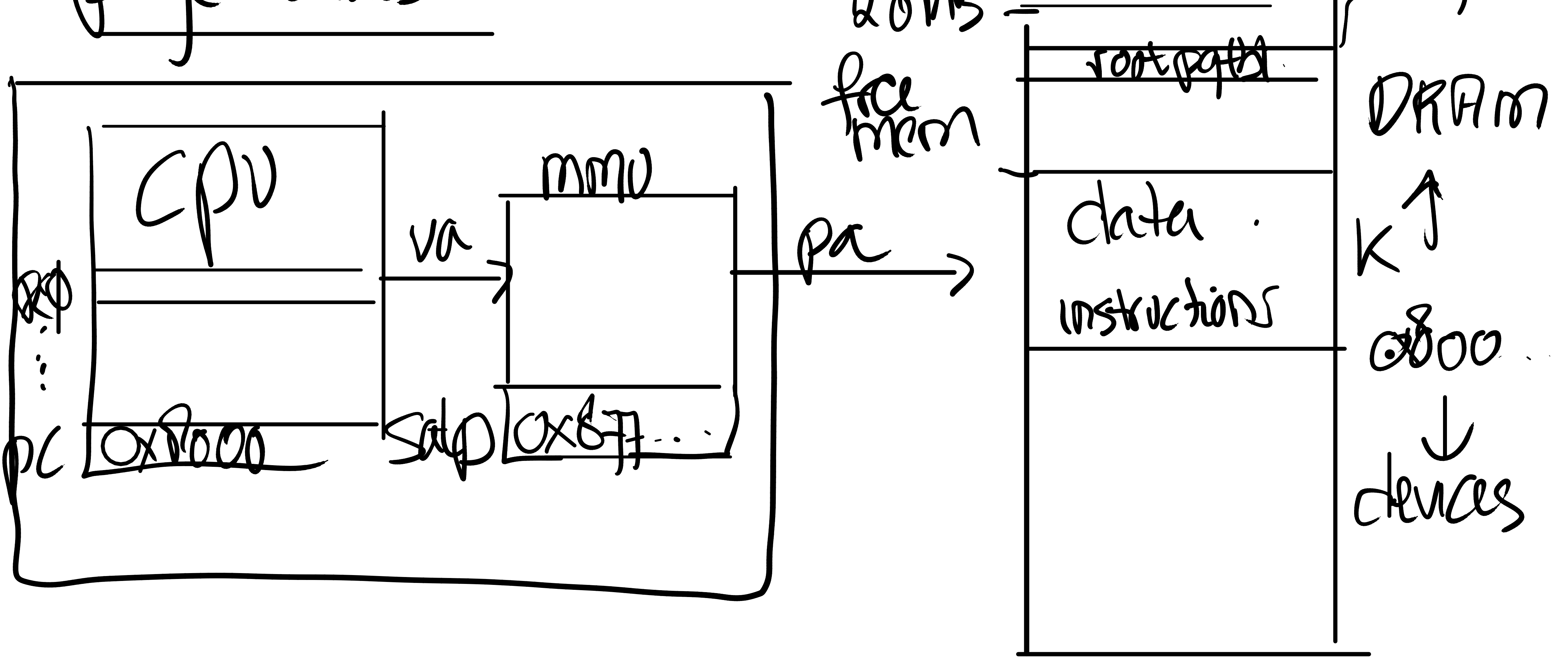
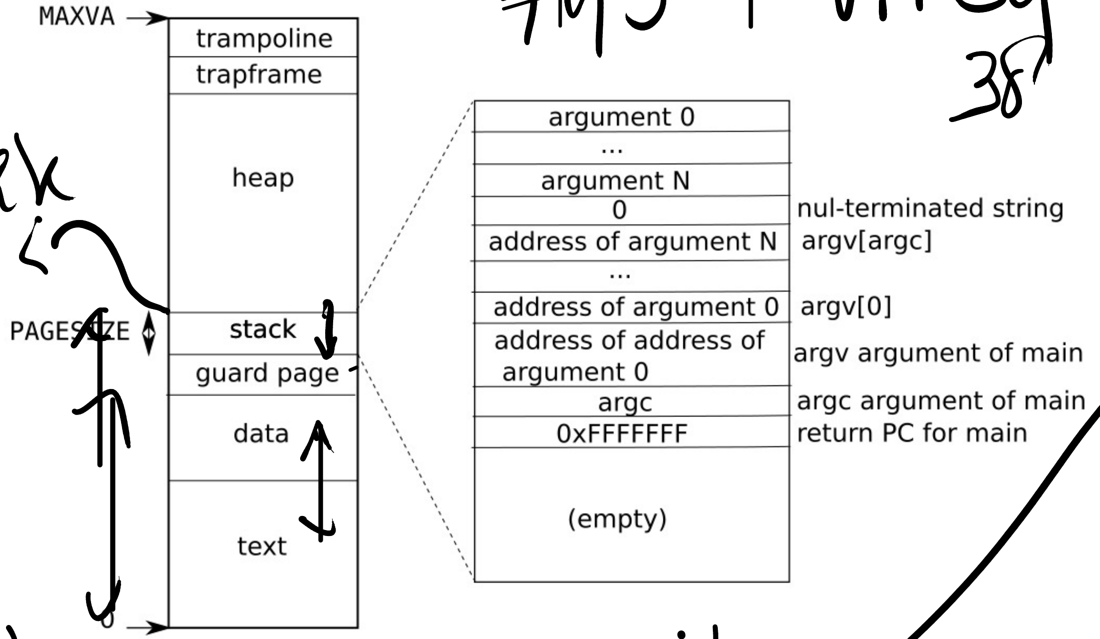
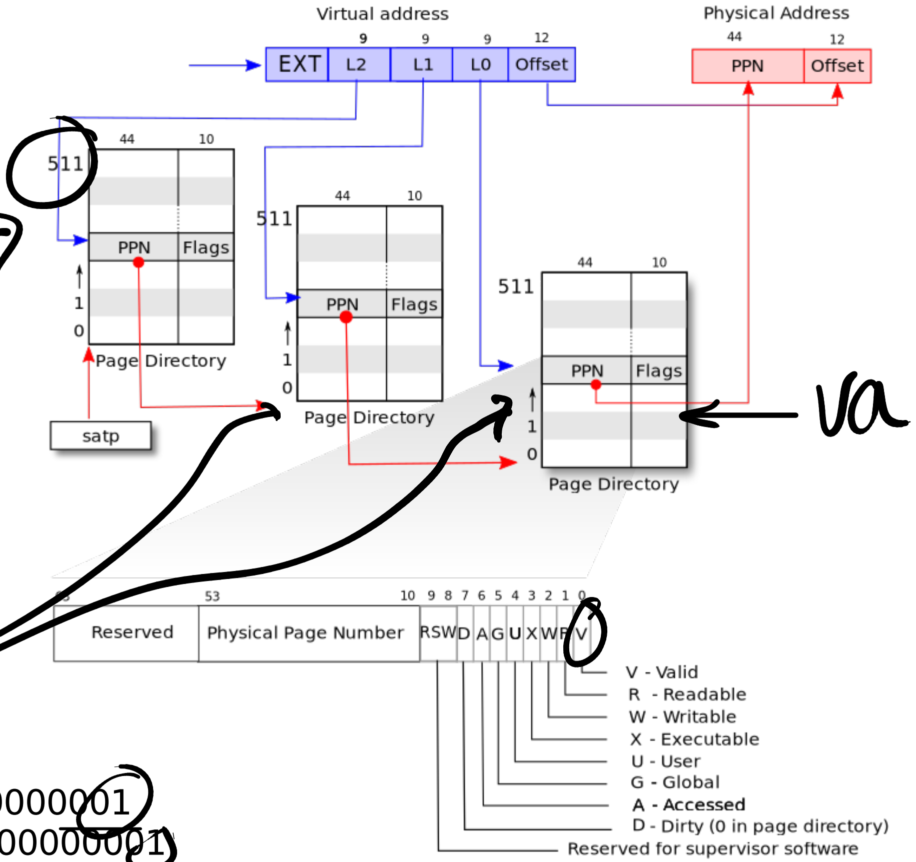

CPU
R0
pc
0x80000
va
MMU
satp
0x877...
pa
128 MB
0x87F...
root pgtbl
free mem
DRAM
data
instructions
K
0x800...
devices

fig3-4 VA 39 ← 38

sbrk



-X)



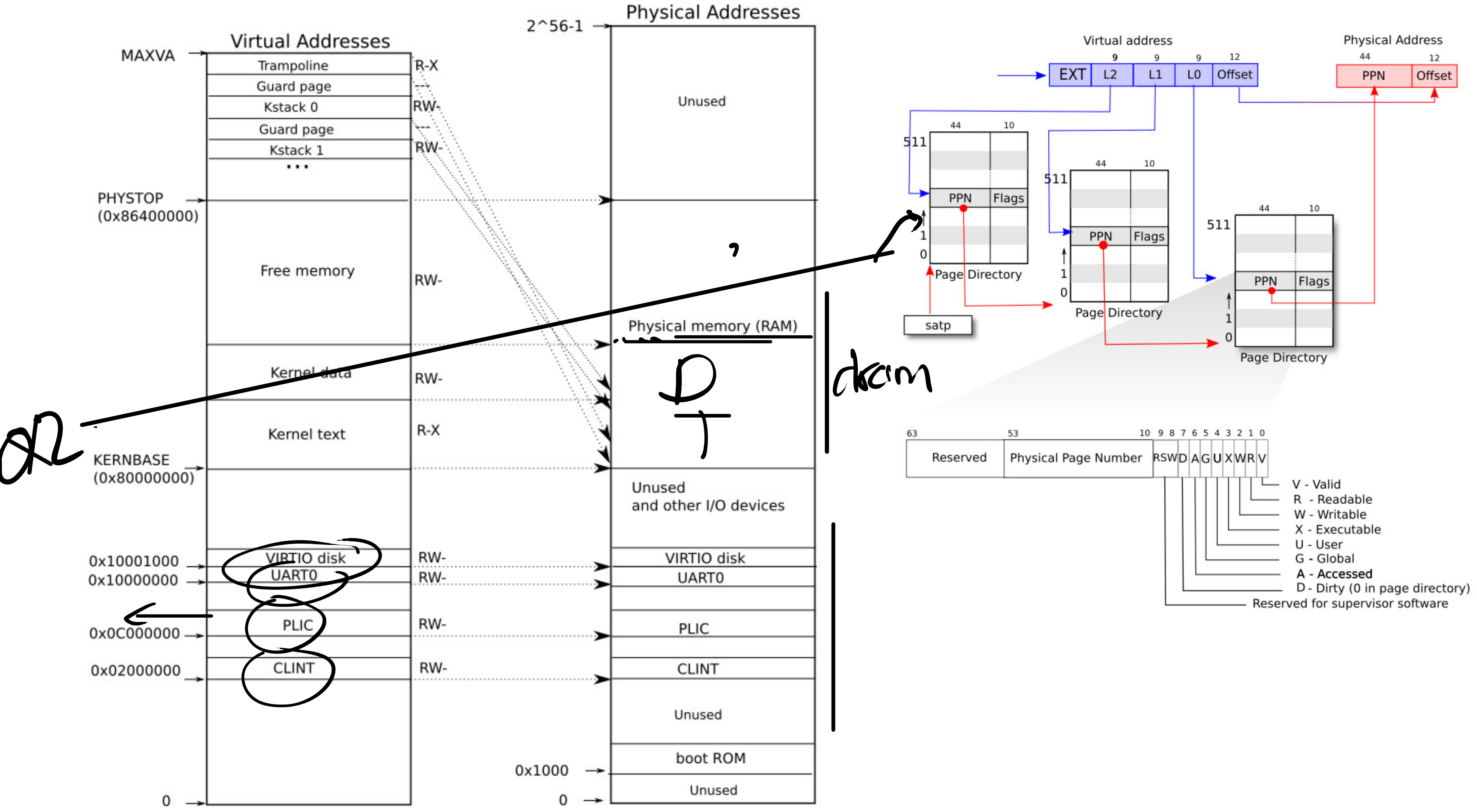
va

init

```
page table 0x0000000087f67000
 ..0: pte 0x0000000021fd8c01 pa 0x0000000087f63000 fl 0x0000000000000001
 .. ..0: pte 0x0000000021fd8801 pa 0x0000000087f62000 fl 0x0000000000000001
 .. .. ..0: pte 0x0000000021fd901f pa 0x0000000087f64000 fl 0x000000000000001f
 .. .. ..1: pte 0x0000000021fd840f pa 0x0000000087f61000 fl 0x000000000000000f
 .. .. ..2: pte 0x0000000021fd801f pa 0x0000000087f60000 fl 0x000000000000001f
 ..255: pte 0x0000000021fd9801 pa 0x0000000087f66000 fl 0x0000000000000001
 .. ..511: pte 0x0000000021fd9401 pa 0x0000000087f65000 fl 0x0000000000000001
 .. .. ..510: pte 0x0000000021fdd807 pa 0x0000000087f76000 fl 0x0000000000000007
 .. .. ..511: pte 0x0000000020001c0b pa 0x0000000080007000 fl 0x000000000000000b
```

RWV

XV


Virtual Addresses
MAXVA
Trampoline
R-X
Guard page

Kstack 0
RW-
Guard page

Kstack 1
RW-
...
PHYSTOP
(0x86400000)
Free memory
RW-
Kernel data
RW-
Kernel text
R-X
KERNBASE
(0x80000000)
0x10001000
VIRTIO disk
RW-
0x10000000
UART0
RW-
0x0C000000
PLIC
RW-
0x02000000
CLINT
RW-
0
Physical Addresses
2^56-1
Unused
Physical memory (RAM)
Unused
and other I/O devices
VIRTIO disk
UART0
PLIC
CLINT
Unused
boot ROM
0x1000
Unused
0
dram
Virtual address
EXT
9
L2
9
L1
9
L0
12
Offset
Physical Address
44
PPN
12
Offset
44
10
511
PPN
Flags
1
0
Page Directory
satp
44
10
511
PPN
Flags
1
0
Page Directory
44
10
511
PPN
Flags
1
0
Page Directory
63
53
10
9
8
7
6
5
4
3
2
1
0
Reserved
Physical Page Number
RSW
D
A
G
U
X
W
R
V
V - Valid
R - Readable
W - Writable
X - Executable
U - User
G - Global
A - Accessed
D - Dirty (0 in page directory)
Reserved for supervisor software

Part 2

Harder than it seems:

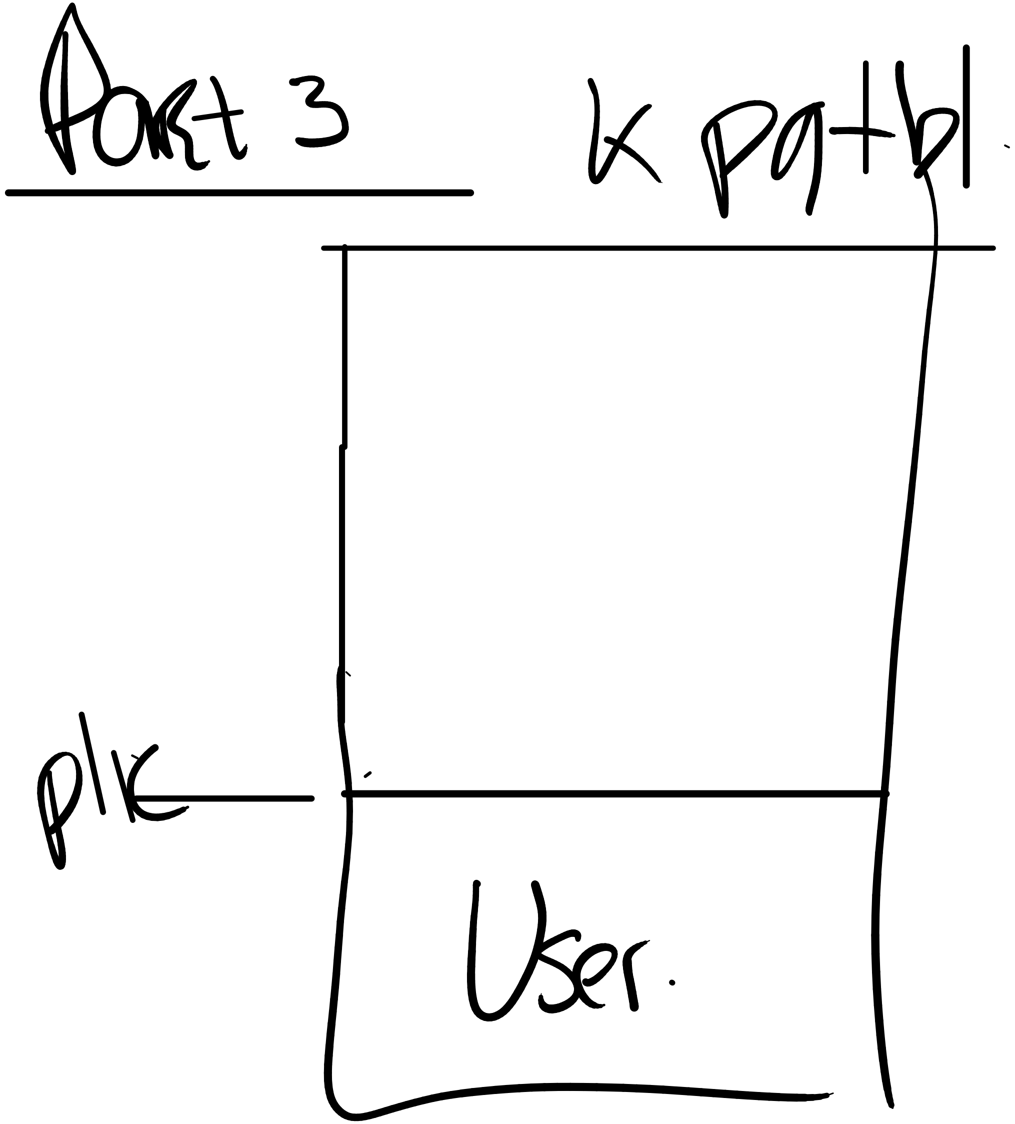
1) xv6 code is specialized for 1 k pgtbl.
2) kvminit() < procinit()
   virtio_disk()
3) cleanup
4) easy-to make error ⇒ hard bug
   ⇒ time consuming to track down.

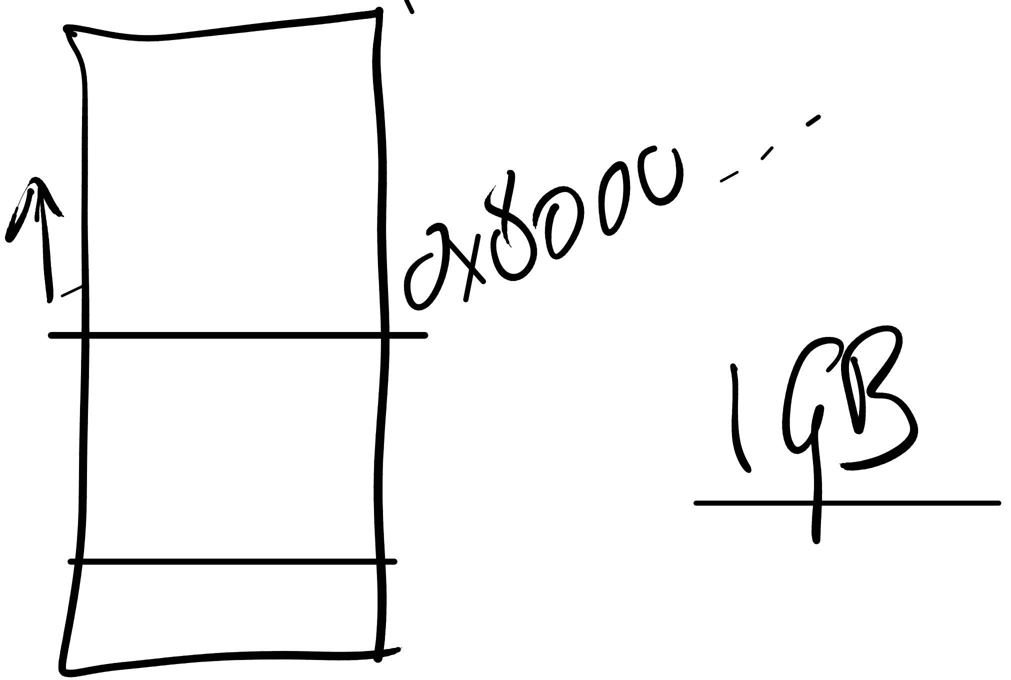
2 Sol approaches

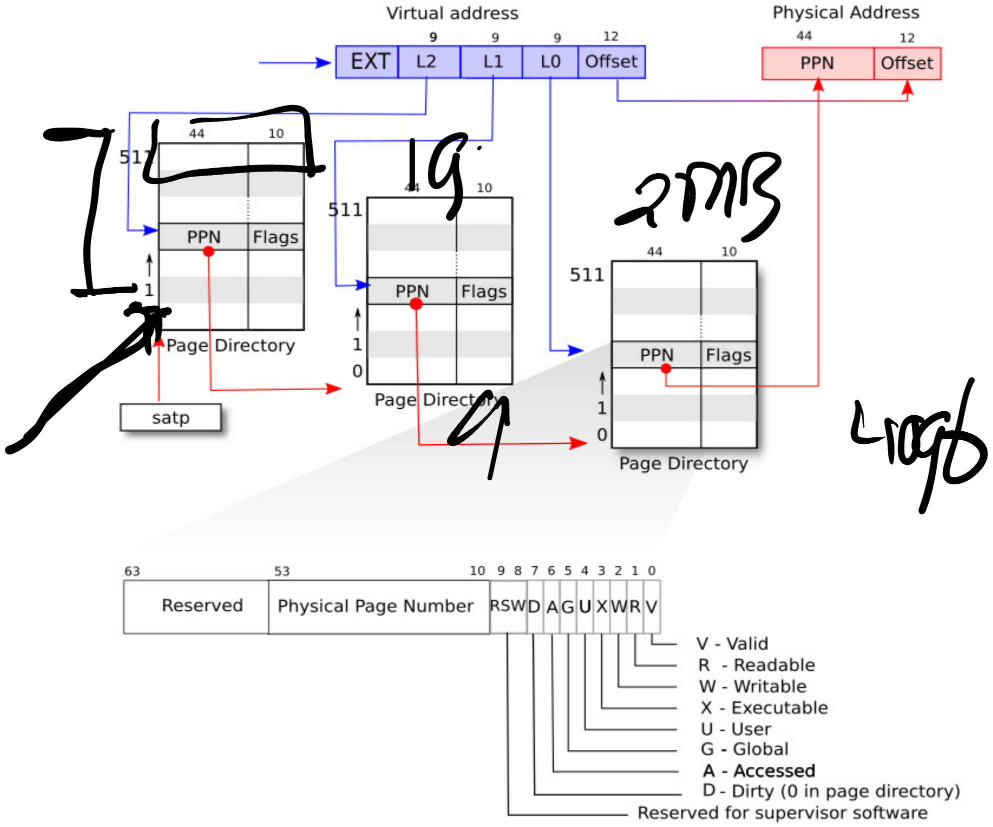
1) copy.
2) share

⇒ baby steps
keep existing code

Part 3

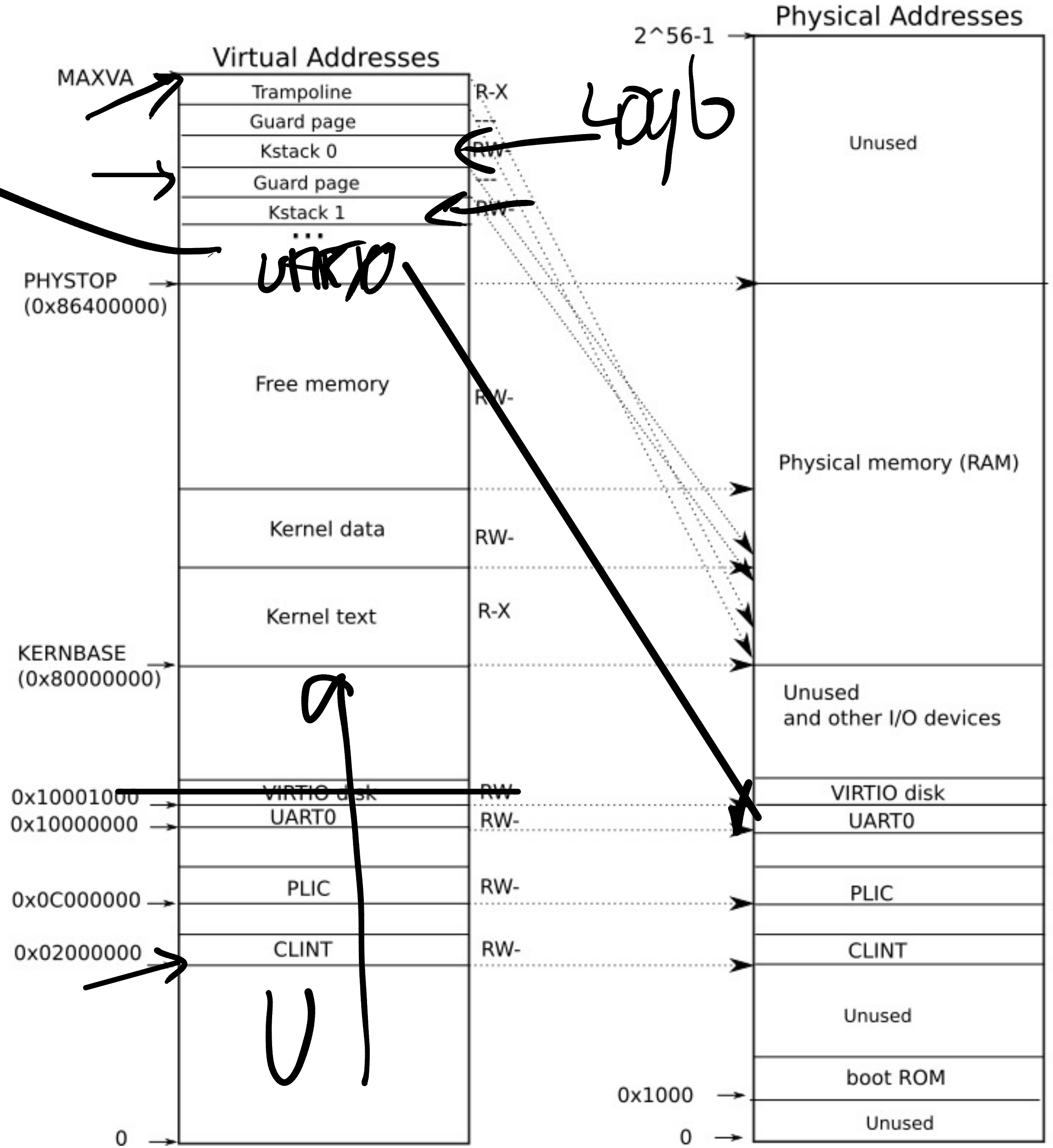






```
page table 0x0000000087f67000
 ..0: pte 0x0000000021fd8c01 pa 0x0000000087f63000 fl 0x0000000000000001
 .. ..0: pte 0x0000000021fd8801 pa 0x0000000087f62000 fl 0x0000000000000001
 .. .. ..0: pte 0x0000000021fd901f pa 0x0000000087f64000 fl 0x000000000000001f
 .. .. ..1: pte 0x0000000021fd840f pa 0x0000000087f61000 fl 0x000000000000000f
 .. .. ..2: pte 0x0000000021fd801f pa 0x0000000087f60000 fl 0x000000000000001f
 ..255: pte 0x0000000021fd9801 pa 0x0000000087f66000 fl 0x0000000000000001
 .. ..511: pte 0x0000000021fd9401 pa 0x0000000087f65000 fl 0x0000000000000001
 .. .. ..510: pte 0x0000000021fdd807 pa 0x0000000087f76000 fl 0x0000000000000007
 .. .. ..511: pte 0x0000000020001c0b pa 0x0000000080007000 fl 0x000000000000000b
```

Linux
meltdown
KPTI


Virtual Addresses
MAXVA
Trampoline
R-X
Guard page

Kstack 0
RW-
Guard page

Kstack 1
RW-
...
4gb
UART0
PHYSTOP
(0x86400000)
Free memory
RW-
Kernel data
RW-
Kernel text
R-X
KERNBASE
(0x80000000)
9
~~VIRTIO disk~~
RW-
0x10001000
0x10000000
UART0
RW-
PLIC
RW-
0x0C000000
CLINT
RW-
0x02000000
U
0
Physical Addresses
2^56-1
Unused
Physical memory (RAM)
Unused
and other I/O devices
VIRTIO disk
UART0
PLIC
CLINT
Unused
boot ROM
0x1000
Unused
0