# Midterm notes about virtual memory

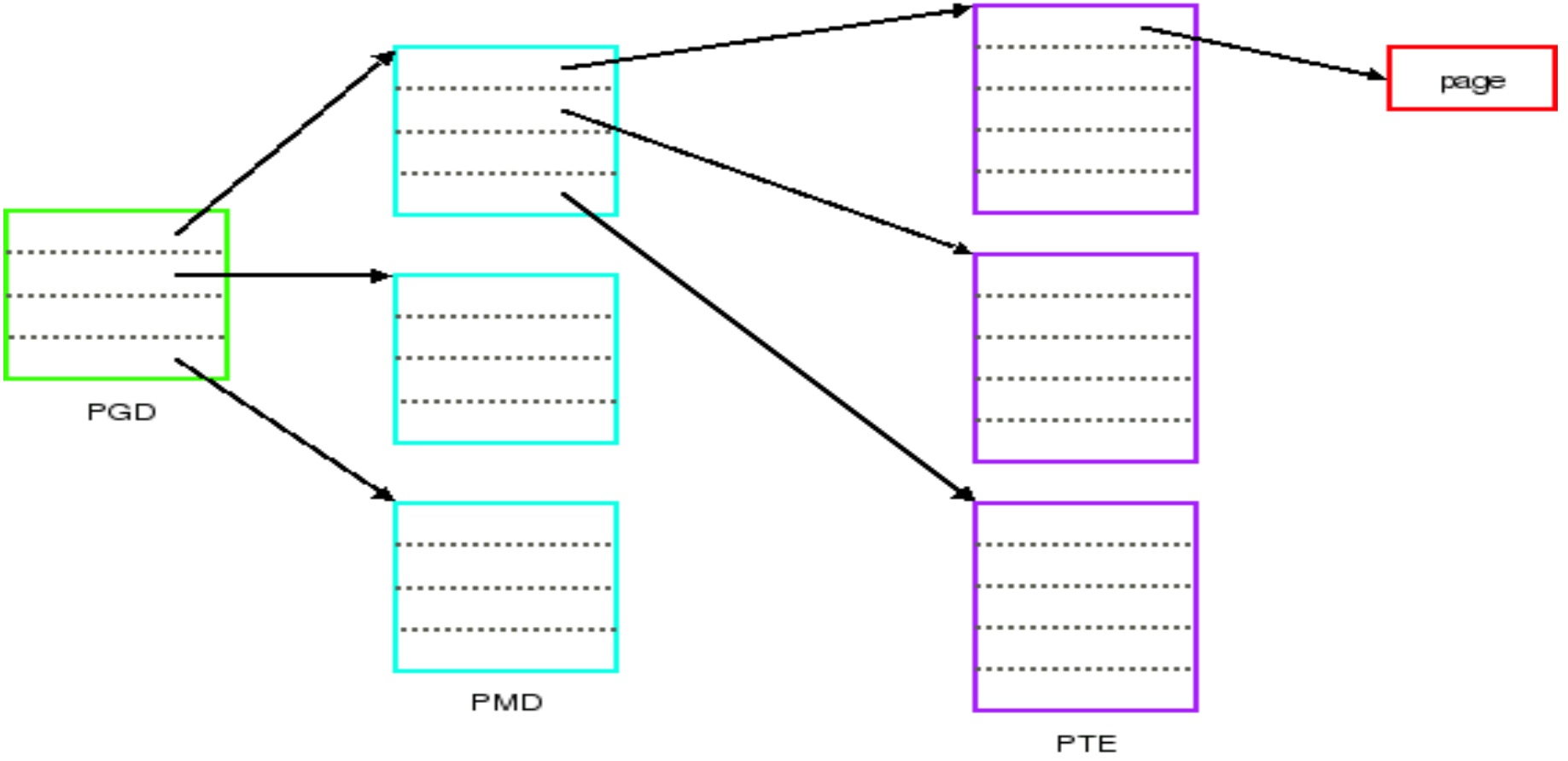
# Rowhammer steps 1 and 2

- What a process thinks is its virtual address space may be mixed up all over physical memory and the disk
- Pages are given to processes by the kernel *lazily*
  - If a process malloc()s a bunch of memory and doesn’t use a special option, no physical pages or page tables exist there until the process starts page faulting

```
jedi@tortuga:~$ head -n 16 /proc/`echo $$`/maps | sed "s/   / /g"
5eb8e1d11000-5eb8e1d40000 r--p 00000000 fc:01 72220755       /usr/bin/bash
5eb8e1d40000-5eb8e1e1f000 r-xp 0002f000 fc:01 72220755       /usr/bin/bash
5eb8e1e1f000-5eb8e1e59000 r--p 0010e000 fc:01 72220755       /usr/bin/bash
5eb8e1e5a000-5eb8e1e5e000 r--p 00148000 fc:01 72220755       /usr/bin/bash
5eb8e1e5e000-5eb8e1e67000 rw-p 0014c000 fc:01 72220755       /usr/bin/bash
5eb8e1e67000-5eb8e1e72000 rw-p 00000000 00:00 0
5eb8e2c62000-5eb8e2e09000 rw-p 00000000 00:00 0          [heap]
739311400000-739312306000 r--p 00000000 fc:01 72221250       /usr/lib/locale/locale-archive
739312400000-739312428000 r--p 00000000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
739312428000-7393125bd000 r-xp 00028000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
7393125bd000-739312615000 r--p 001bd000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
739312615000-739312616000 ---p 00215000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
739312616000-73931261a000 r--p 00215000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
73931261a000-73931261c000 rw-p 00219000 fc:01 72286240       /usr/lib/x86_64-linux-gnu/libc.so.6
73931261c000-739312629000 rw-p 00000000 00:00 0
7393127fc000-7393127ff000 rw-p 00000000 00:00 0
```

# Rowhammer step 3

- Multi-level page tables save physical memory (by having less page tables) as long as a process doesn’t spread its memory all over its virtual address space
  - Can even page the page tables




https://lwn.net/Articles/106177/

# Rowhammer steps 4 and 5

- If a file is mapped into virtual memory over and over again, in the same process or in different processes, the kernel puts only one copy of it in physical memory
  - Unless Copy-on-Write (CoW) happens
- The kernel keeps its own records about what's mapped and the permissions
  - Assumes that it's safe in step #5 of rowhammer to use that physical page for a "rx" mapping of the ping code

# About MELTDOWN

- Precise interrupts are a *must* for modern commodity OSes
- Kernel Page-Table Isolation (KPTI)
  - Kernel and processes can no longer share page tables