TWICE

Row hammer attack:

→ aggressor row

→ victim rows

Read section 2.2

Read section 3 for RH attack

→ Counters in RCD, not memory controller

↳ Even if DIMMs are empty, then we should still maintain Counter.

$tREFW$: Refresh window

Each row must be refreshed once.

$tREFI$: Refresh interval → ?

$tRFC$: Refresh command → ?

tRC : Read cycle time → Perform one act

th_{RH} : RH detection threshold

th PI : Pruning interval threshold.

- Total acts possible per refresh period = $\frac{tREFW}{tRC}$
- Total aggressor rows per refresh period = $\frac{tREFW}{tRC \times N_{th}}$

N_{th} = # acts for a guaranteed bit flip

- Total victim rows = $\frac{2\ tREFW}{tRC \times N_{th}}$

$th_{RH} < N_{th}$.

- Only 20 rows can be exposed to RH attack from a bank in the duration tREFW

→ So we need only 20 counters.

→ th PI → Remove if not act within this

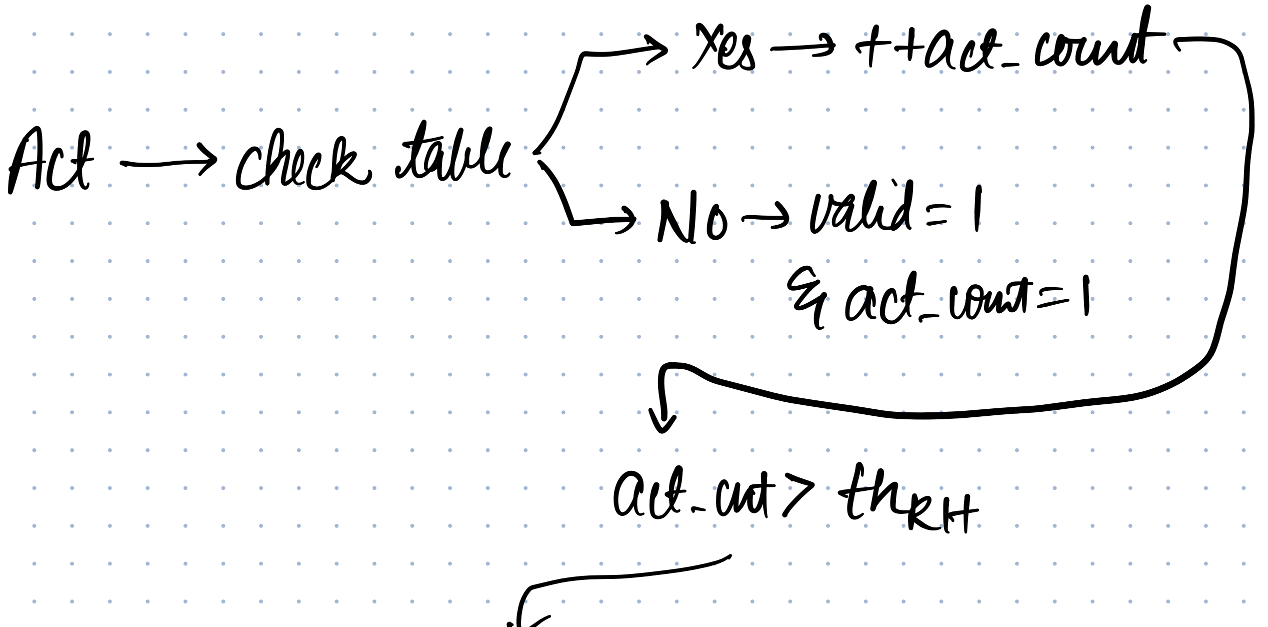
valid	row_addr	act_cnt	life

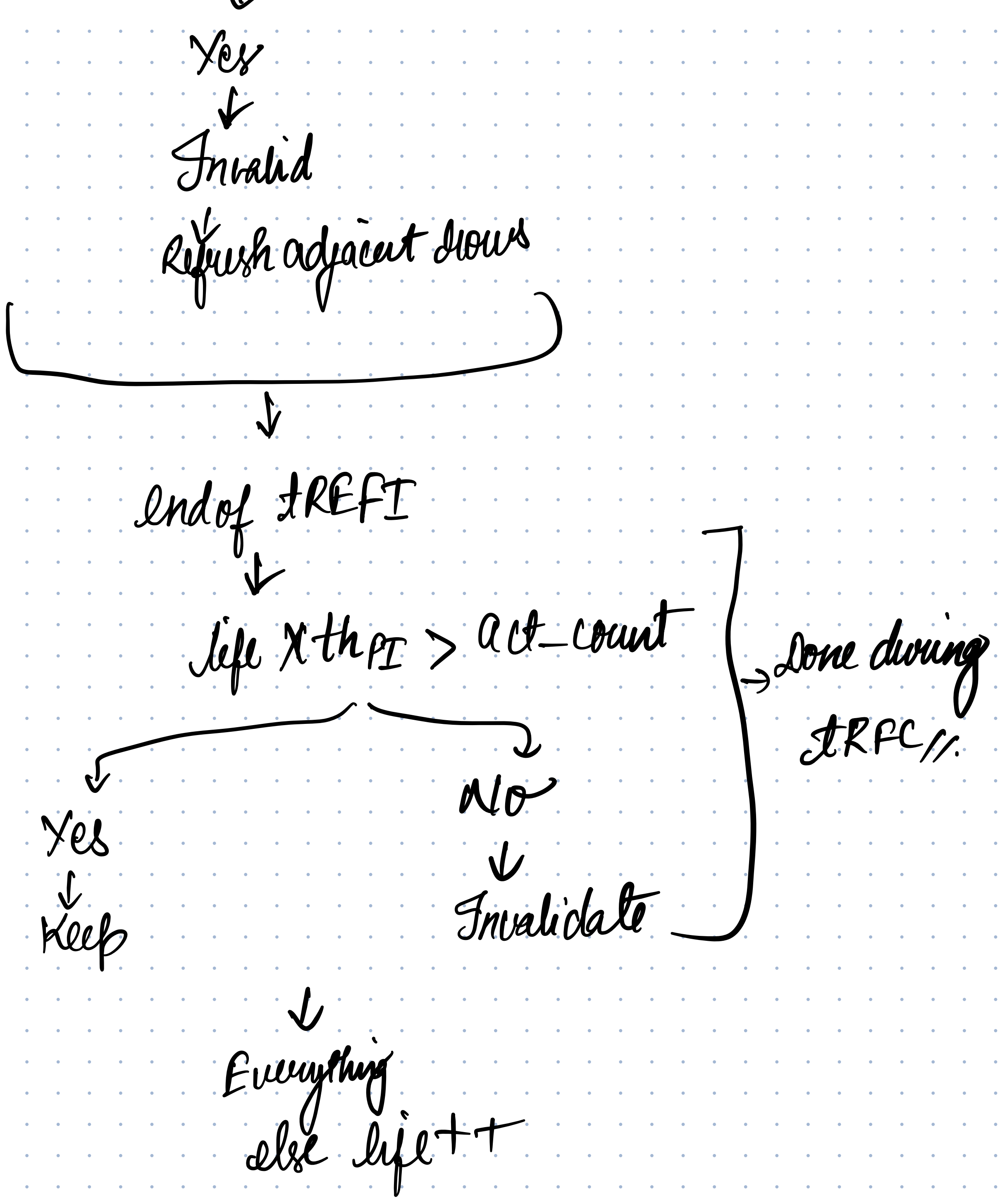
→ Each row must be refreshed once every tREFW

→ For successful attack, Act > thRH within tREFW

$$th_{PI} = \frac{th_{RH}}{\boxed{tREFW/tREFI}}$$

→ How many acts can be done in tREFW if each act takes tREFI.





Correctness of tWiCE:

Proof of RH prevention:

The number of acts to each row over tREF W cannot exceed the thRH without being detected.

count$_{not\_track}$ → Max act without getting detected.

Retain in table → act cnt $\geq th_{PI} \times life$

count_not track → must be less than $th_{PI} \times life$.

Life over refresh window $= \dfrac{tREFW}{tREFI}$

$$th_{PI} = \frac{th_{RH}}{tREFW/tREFI}$$

$$count_{not\ track} < th_{PI} \times \frac{tREFW}{tREFI} = th_{RH}$$

$$max_{life} = \frac{tREFW}{tREFI}$$

$$th_{PI} = \frac{th_{RH}}{tREFW/tREFI}$$

$$count_{not\_track} < th_{PI} \times life$$

$$< th_{PI} \times \frac{tREFW}{tREFI} = th_{RH}$$

$$count_{not\_track} < th_{RH}$$

$$Count_{track} < th_{RH}$$

$$\text{Combined} = \text{Count}_{not\_track} + \text{Count}_{track} < th_{RH} + th_{RH}$$

Two aggressor →

Doubt: How did we make the jump from this to the 1/2 logic?

Location 1/.

Counter Table size:

$$max_{act} = \frac{tREFI - tRFC}{tRC}$$

Two types entries:

1) Newly inserted in the current PI
2) From previous PI

1) New entries is bounded by max_{act}

2) This I didnt understand fully.