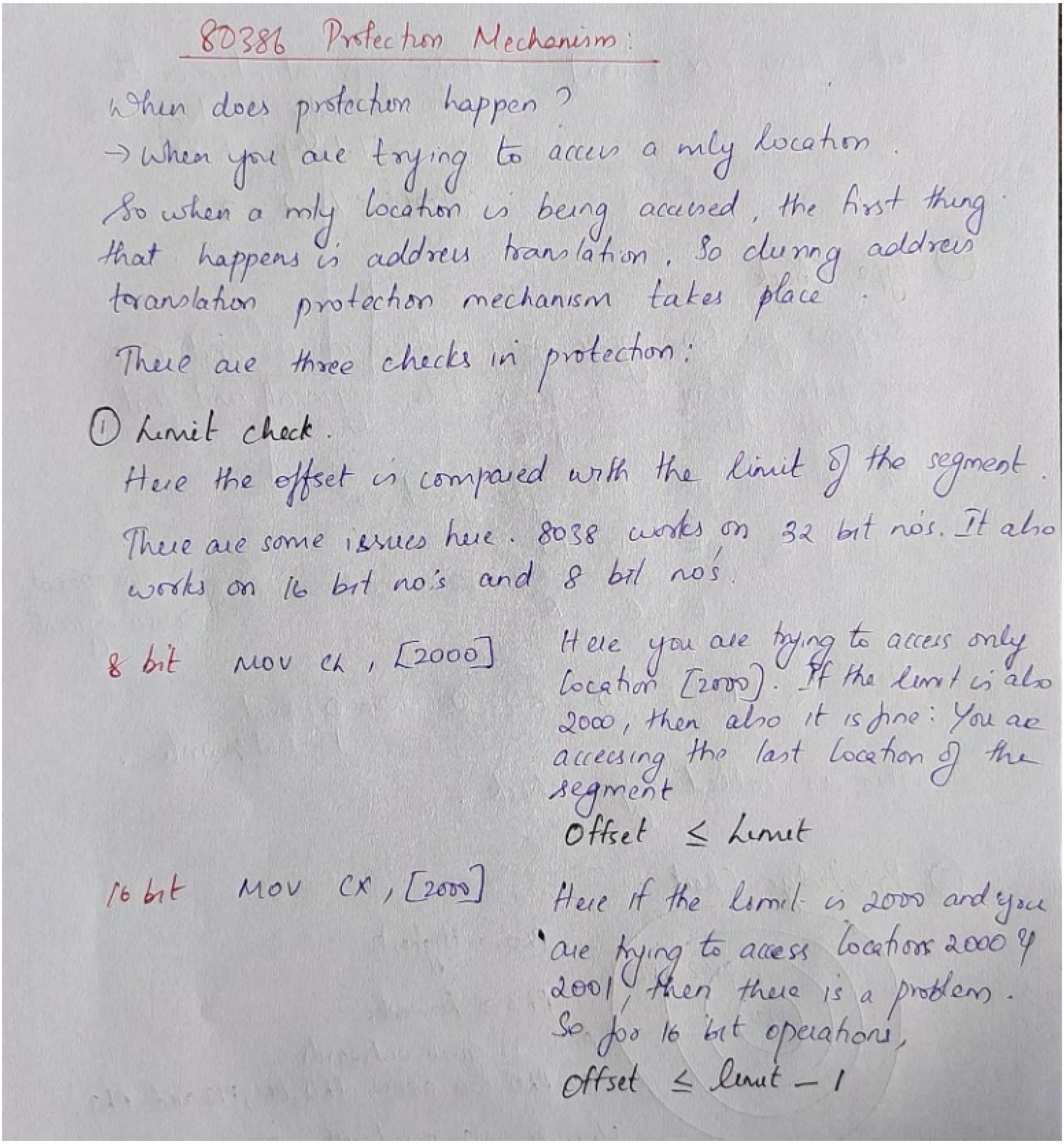


80386 Protection Mechanism:

When does protection happen?

→ When you are trying to access a mly location.

So when a mly location is being accessed, the first thing that happens is address translation. So during address translation protection mechanism takes place.

There are three checks in protection:

① Limit check.

Here the offset is compared with the limit of the segment.

There are some issues here. 8038 works on 32 bit no's. It also works on 16 bit no's and 8 bit no's.

8 bit MOV CL, [2000]

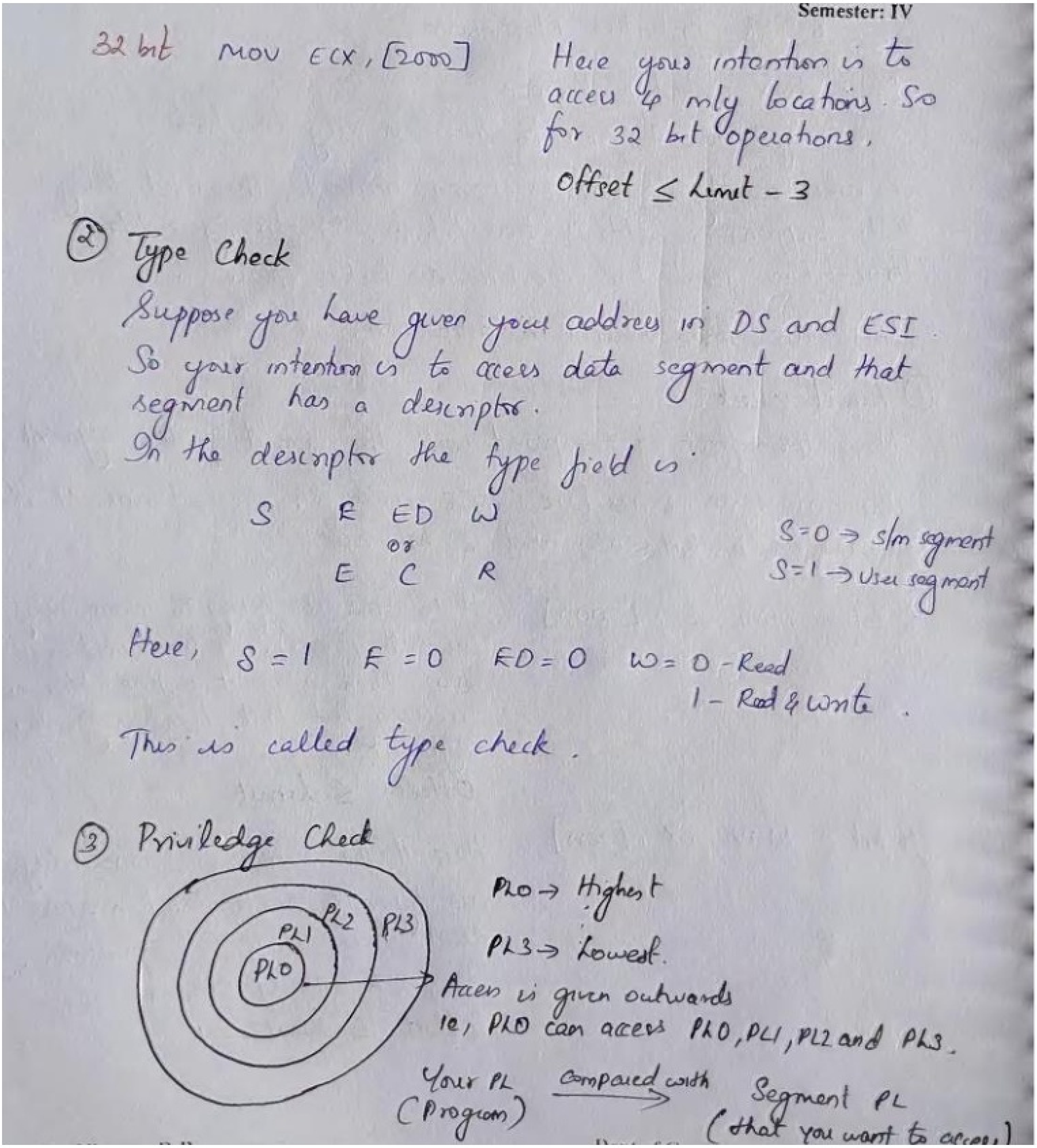
Here you are trying to access only location [2000]. If the limit is also 2000, then also it is fine: You are accessing the last location of the segment

Offset ≤ Limit

16 bit MOV CX, [2000]

Here if the limit is 2000 and you are trying to access locations 2000 & 2001, then there is a problem. So for 16 bit operations,

Offset ≤ limit − 1



Semester: IV

32 bit   MOV ECX, [2000]   Here your intention is to access 4 mly locations. So for 32 bit operations,

Offset ≤ Limit − 3

② Type Check

Suppose you have given your address in DS and ESI. So your intention is to access data segment and that segment has a descriptor.

In the descriptor the type field is:

S   E   ED   W
        or
    E   C   R

S=0 → s/m segment
S=1 → User segment

Here, S = 1   E = 0   ED = 0   W = 0 - Read
1 - Read & write.

This is called type check.

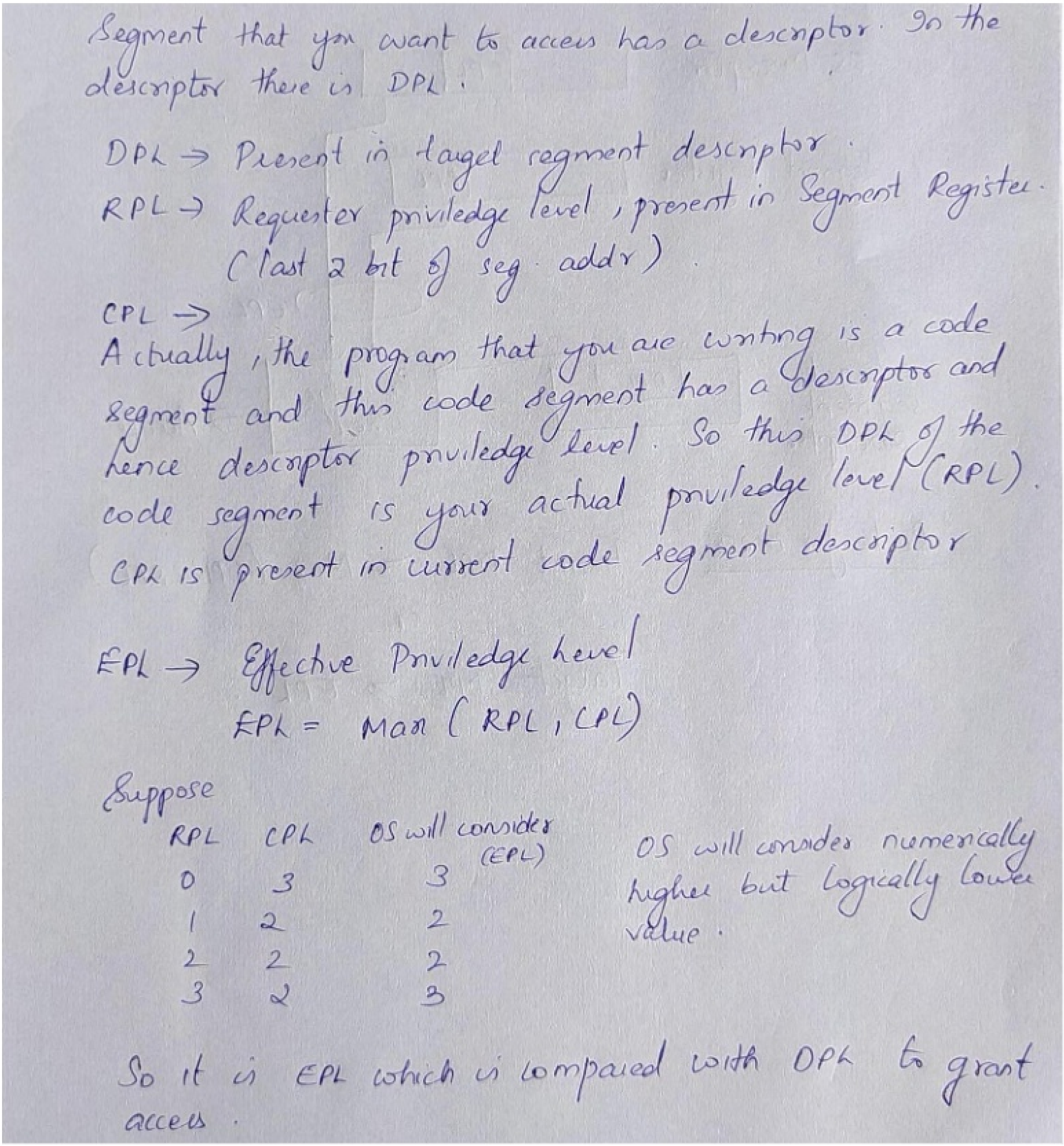
③ Priviledge Check

PL0 → Highest

PL3 → Lowest.

Access is given outwards
ie, PL0 can access PL0, PL1, PL2 and PL3.

Your PL (Program) $\xrightarrow{\text{compared with}}$ Segment PL (that you want to access)



Segment that you want to access has a descriptor. In the descriptor there is DPL.

DPL → Present in target segment descriptor.

RPL → Requester priviledge level, present in Segment Register. (last 2 bit of seg. addr).

CPL →

Actually, the program that you are writing is a code segment and this code segment has a descriptor and hence descriptor priviledge level. So this DPL of the code segment is your actual priviledge level (RPL).

CPL is present in current code segment descriptor

EPL → Effective Priviledge Level

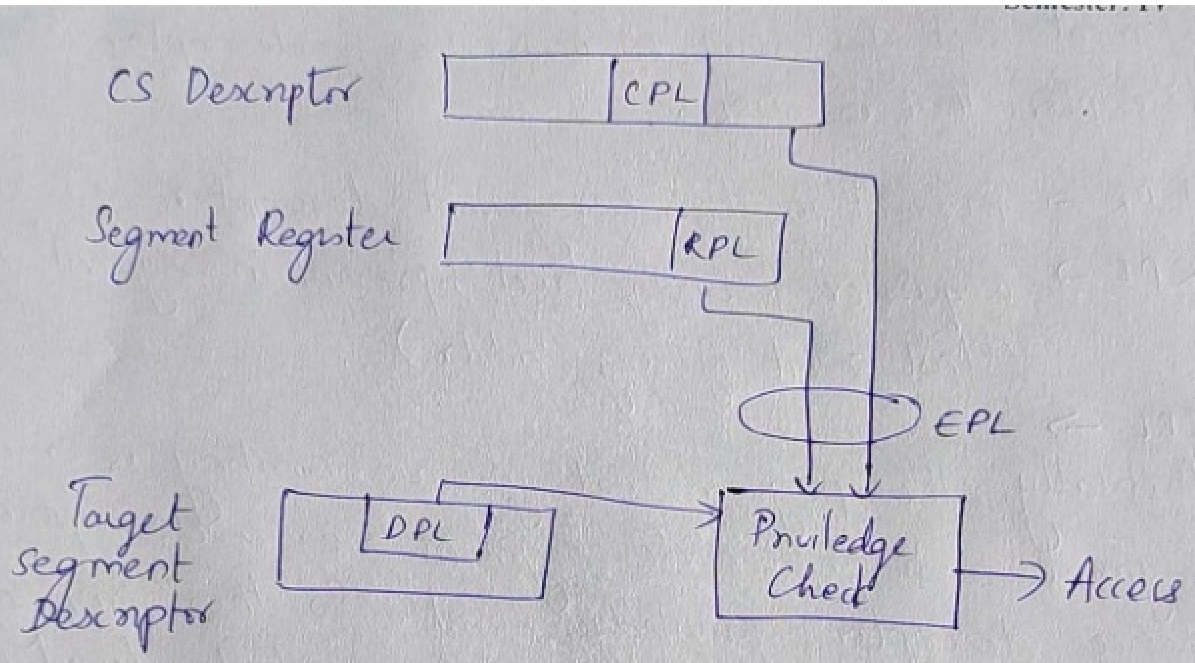
EPL = Max (RPL, CPL)

Suppose

RPL	CPL	OS will consider (EPL)
0	3	3
1	2	2
2	2	2
3	2	3

OS will consider numerically higher but logically lower value.

So it is EPL which is compared with DPL to grant access.



Rule for acces:

Target DPL $\geq$ Max (CPL, RPL)

or

Target DPL $\geq$ EPL.