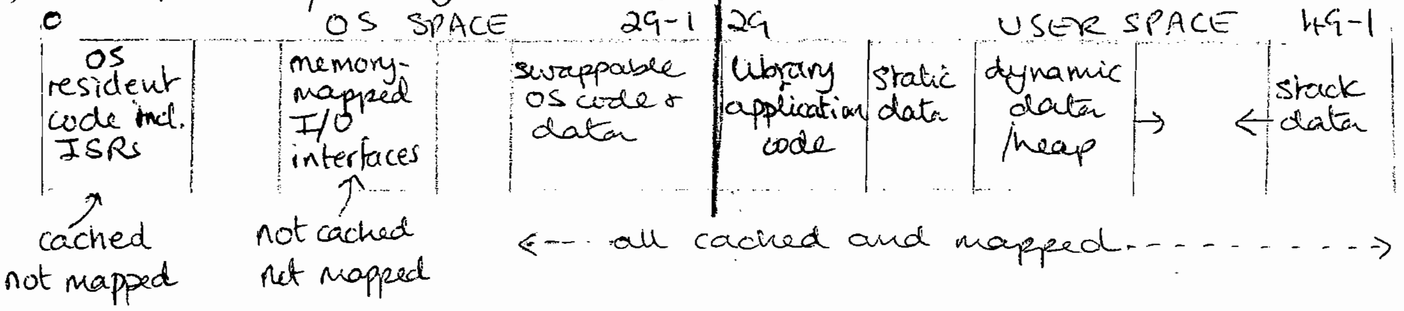
Paper 10 2G/Dip. OS fdns. on end part I and part II intro. memmgt. JMB 2003

a (i) The address range the process can access or transfer control within

(ii) 32-bit add sp: byte 0 → byte 4G−1 $(2^{32}-1)$



different conventions in hardware and software are possible but must be known for cache and TLB management

(iii) • the alternative is to define privileged instructions for I/O which cause an exception when executed from user space

• mem-mapped I/O interfaces are allocated physical addresses the devices listen to the address lines on the bus caching and mapping are meaningless

(iv) OS code is resident so is never relocated. Physical addresses can therefore be used making mapping (i.e. using the TLB with scarce space) unnecessary. Caching is appropriate.

(v) OS addresses can be detected (top bit is 0 or 1 depending on which half of address space is used by convention).
An access or jump to OS space from user space causes a privilege violation.

(vi) A privileged instruction (TRAP) which causes a (software) interrupt is used to implement system calls. The ISR analyses the TRAP and transfers control to the appropriate part of the OS.

b) Multiprogramming became possible
One user's code could be prevented from corrupting the OS (as in (v)) thus affecting other users' operation.
One user's code could not access another user's – only the process address space is visible – not physical addresses.
Hardware support:
At least a base and limit register for relocation and protection loaded for the current process.
Add base to address for relocation
check address now within base → base+limit for protection.
If OK address used for physical memory access. (DIAGRAM).
In practice – 2 pairs allow one segment to be shared (eg execute-only code) and a second to be private. DOS on 8086 has 4 pairs.
Address must then be a tuple (segment#, offset)

10