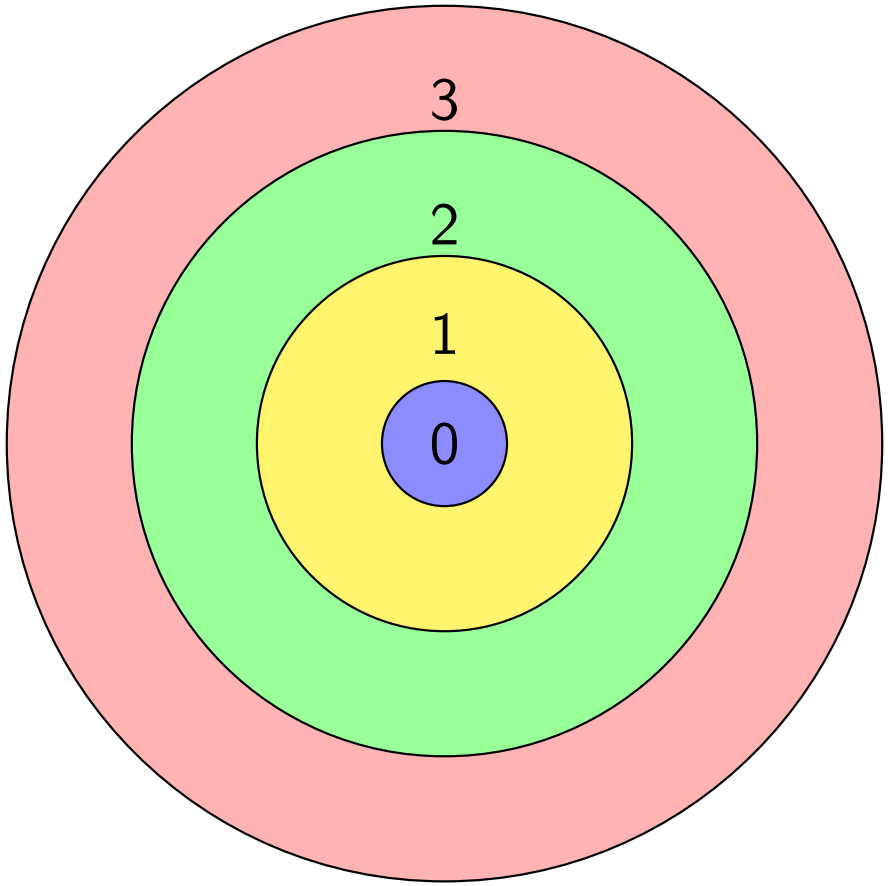
SCS1312 Operating System Concepts

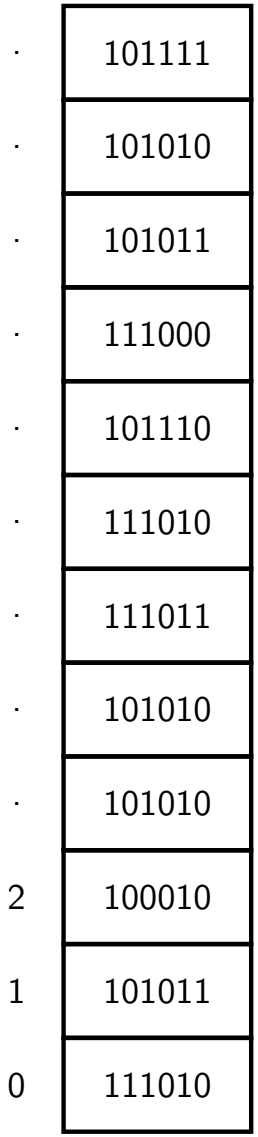
Dr. Chamath Keppitiyagama

University of Colombo School of Computing

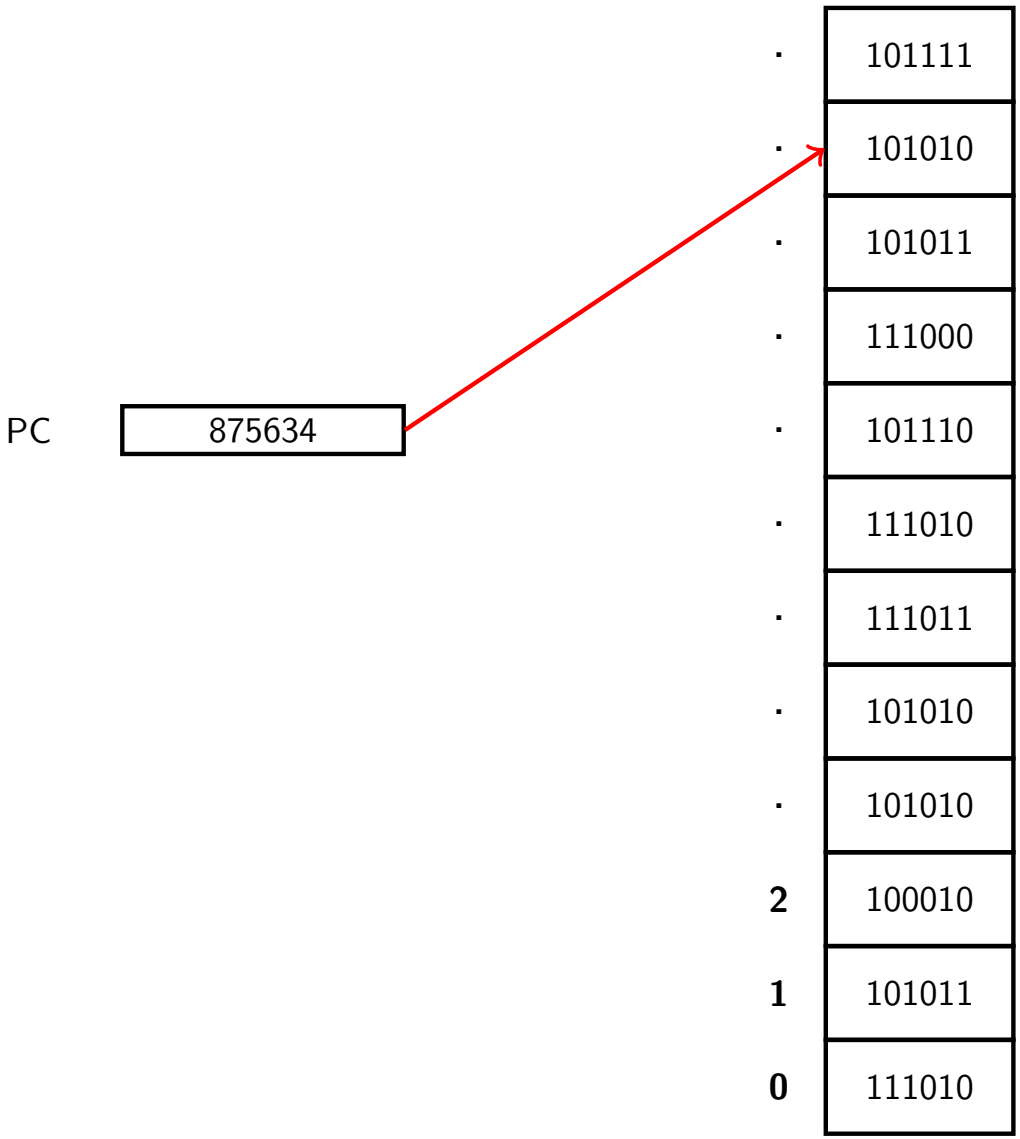
x86 Rings



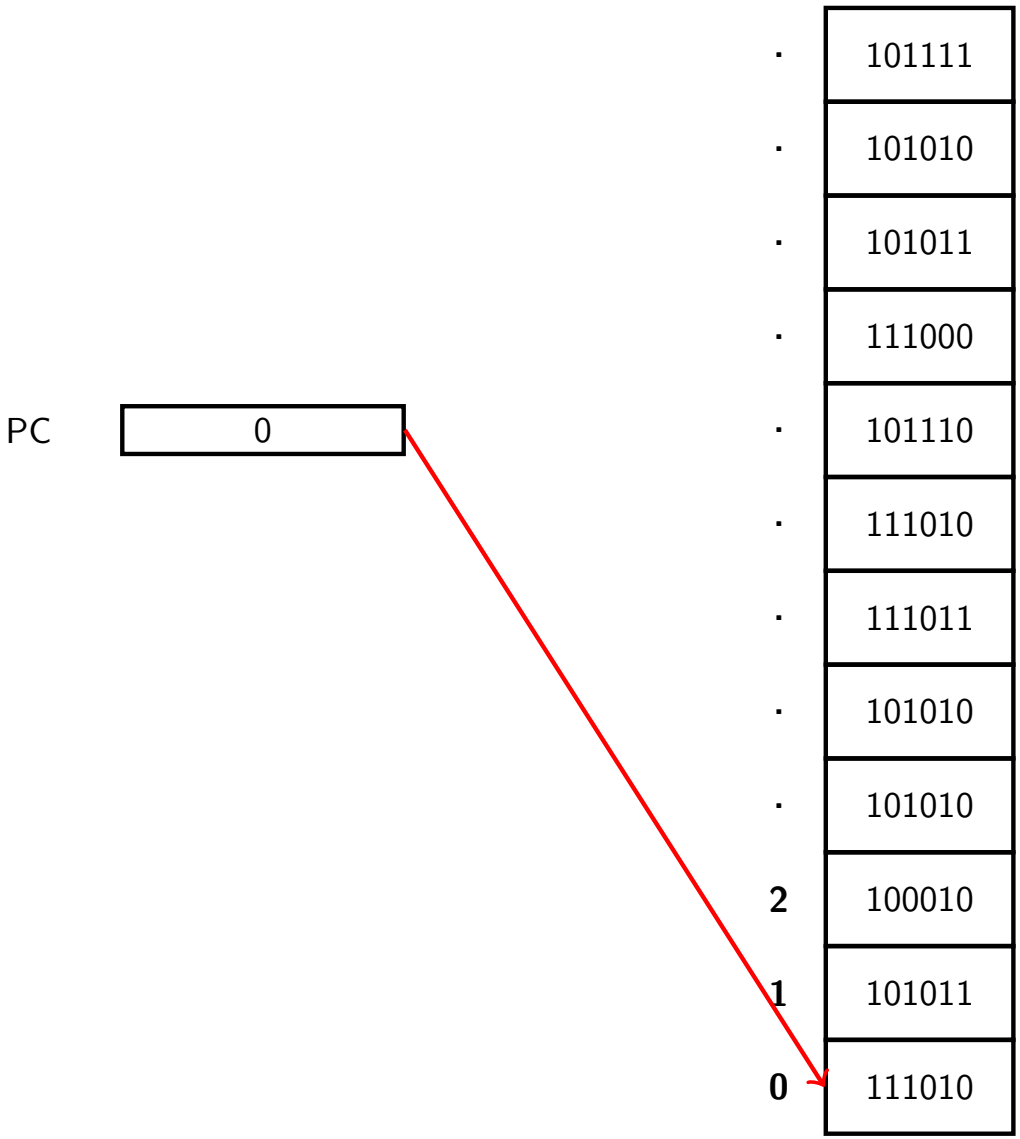
At the Beginning . . .



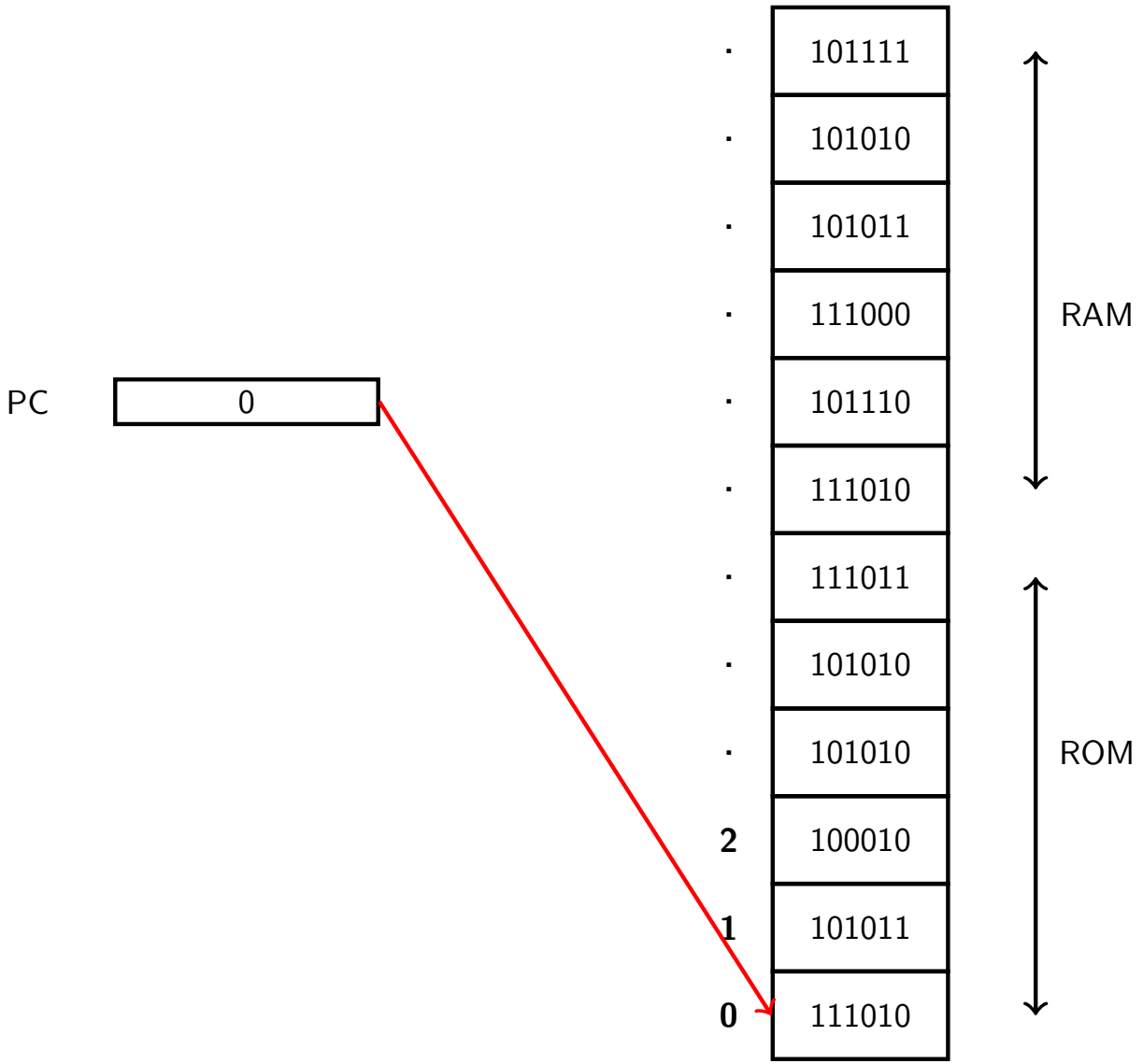
PC ??


PC
875634
101111
101010
101011
111000
101110
111010
111011
101010
101010
100010
101011
111010
2
1
0

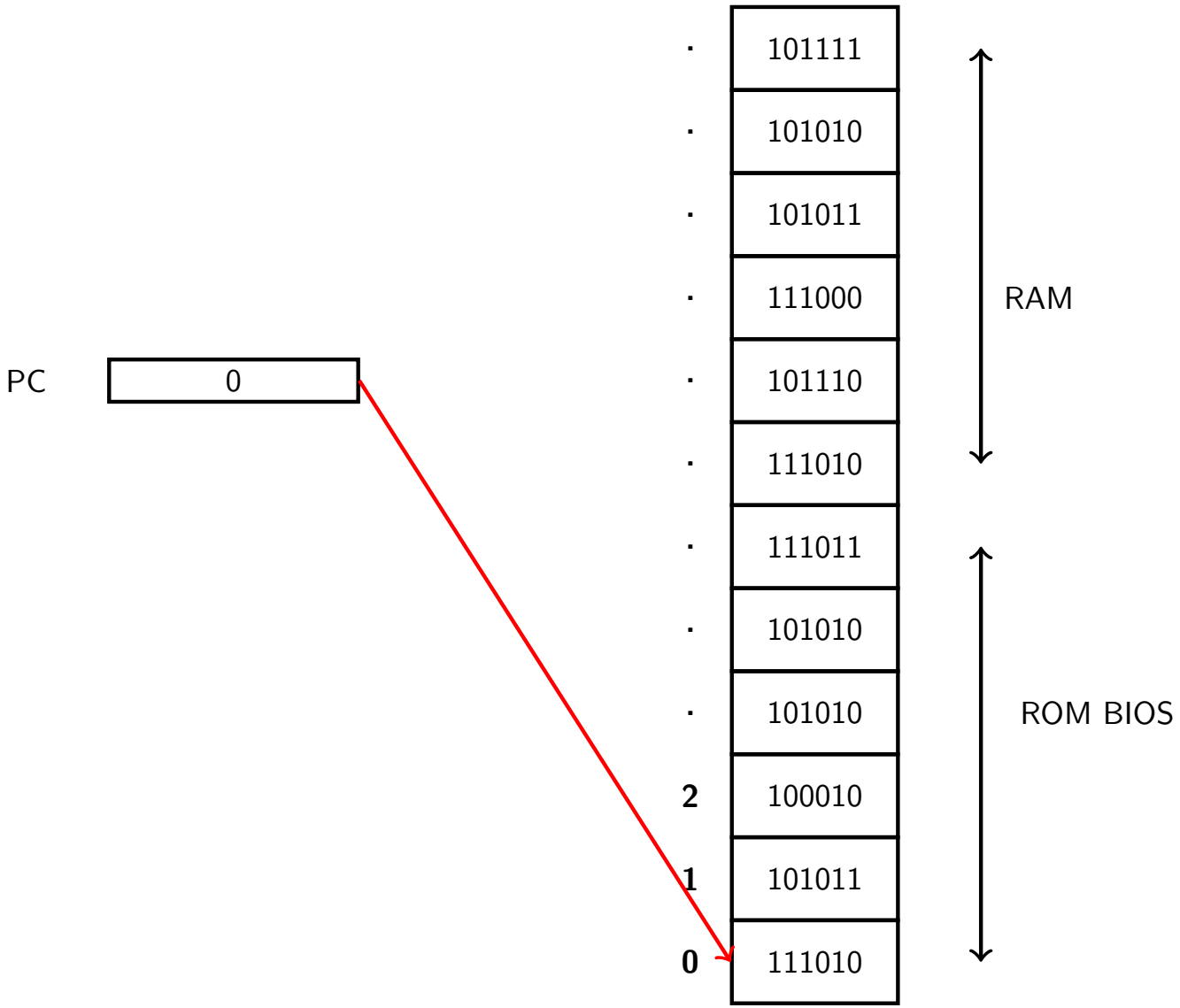
Hard Coded PC



Hard Coded PC



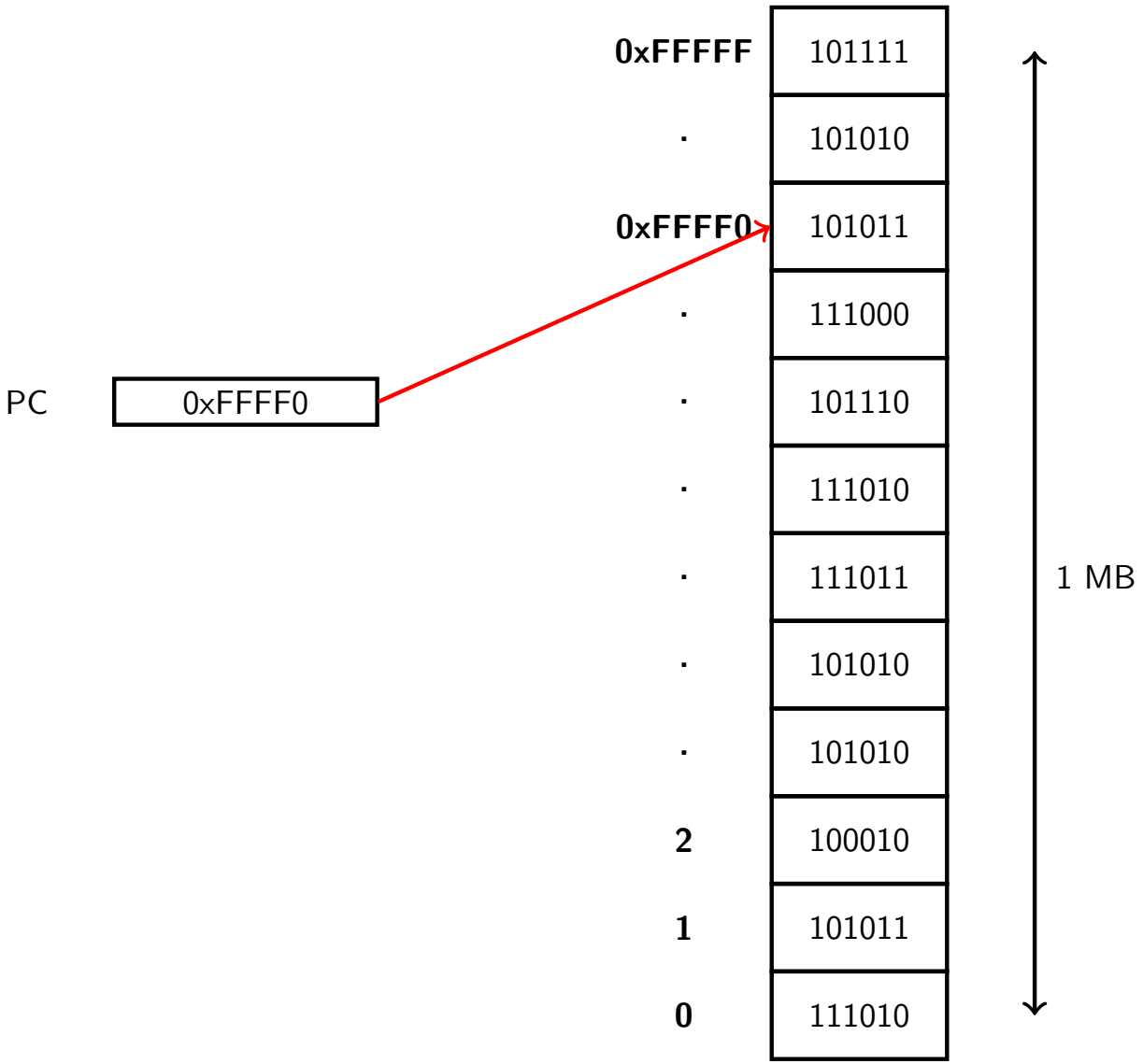
Basic Input Output System - BIOS

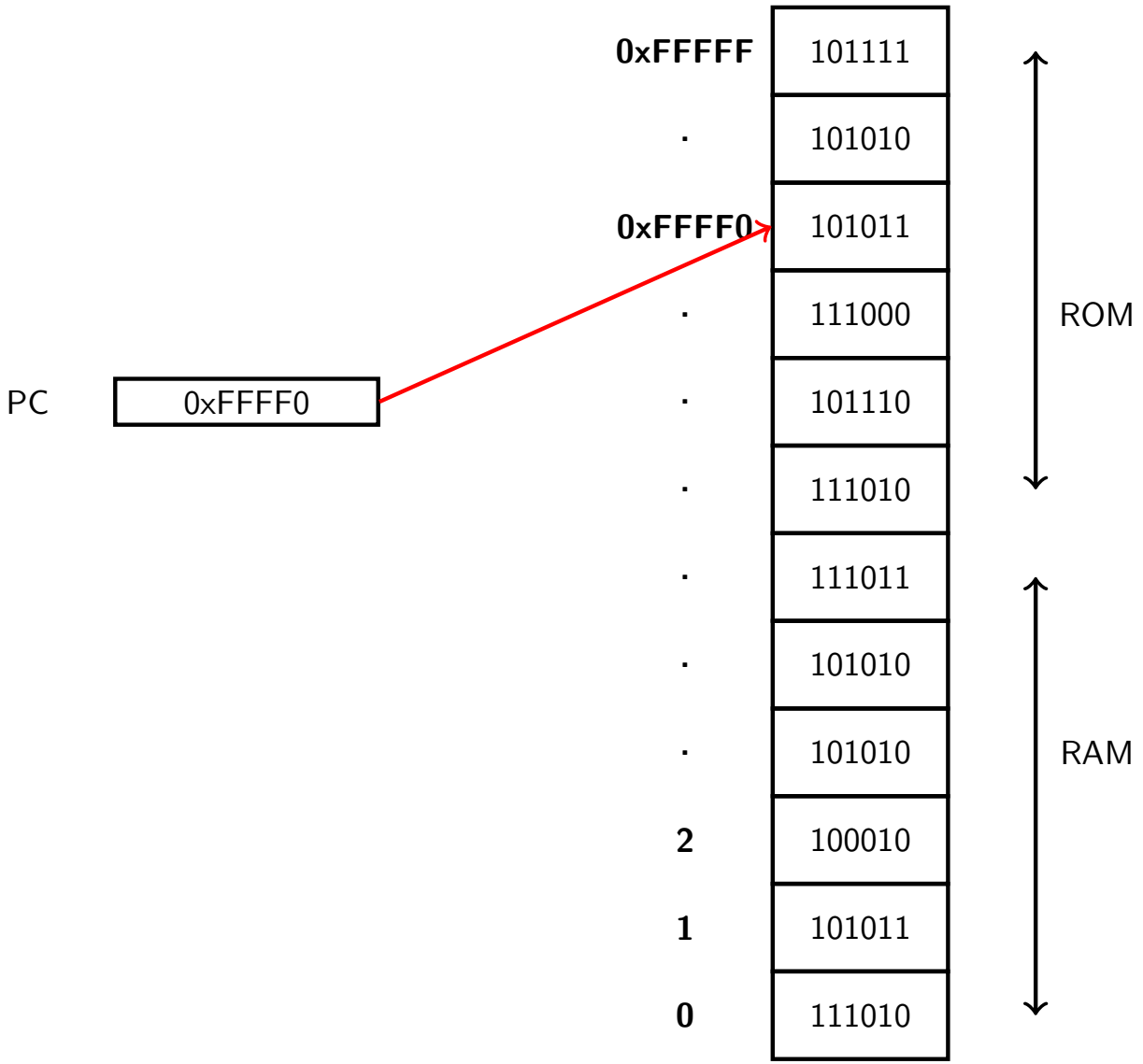


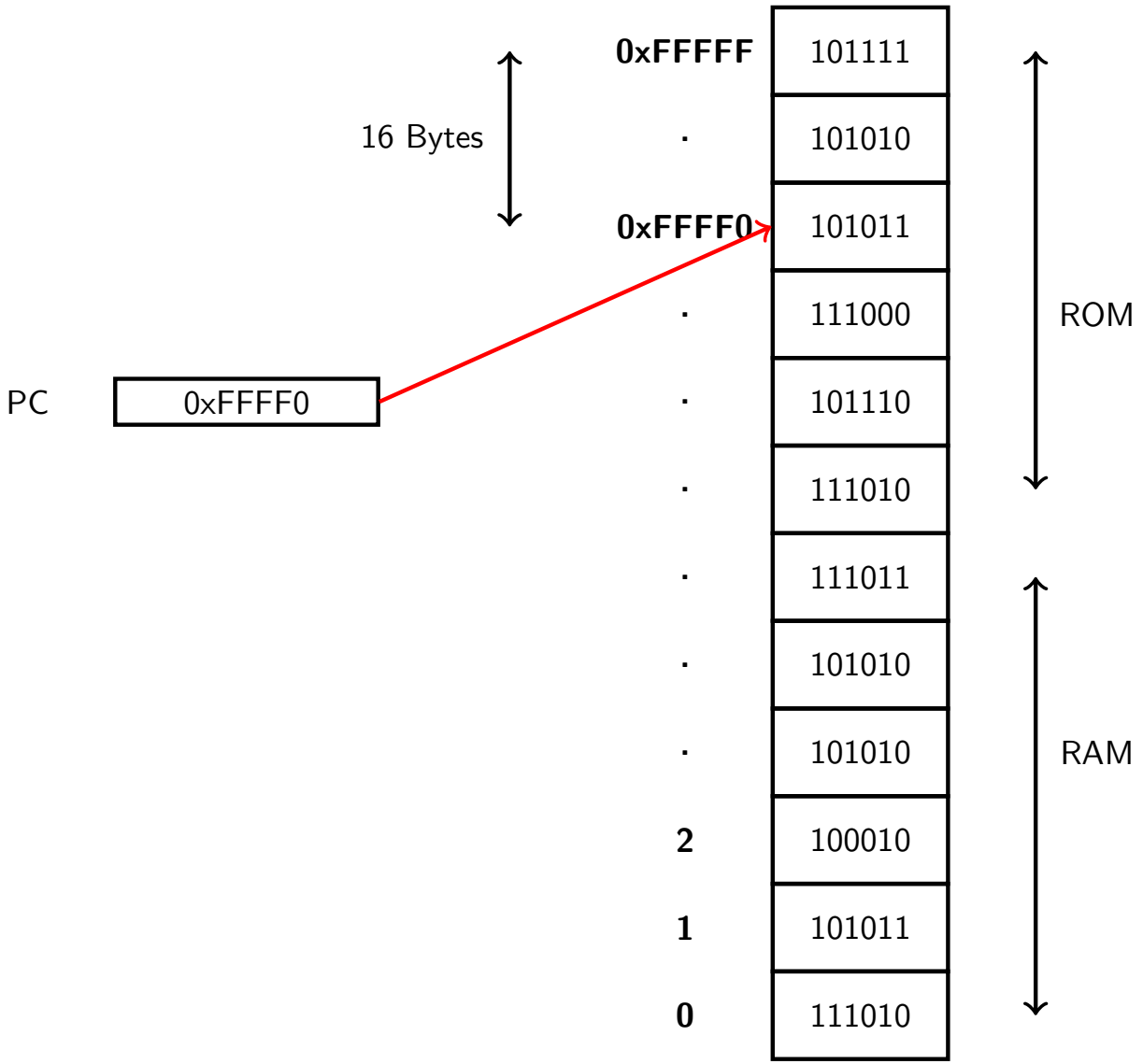
Quiz

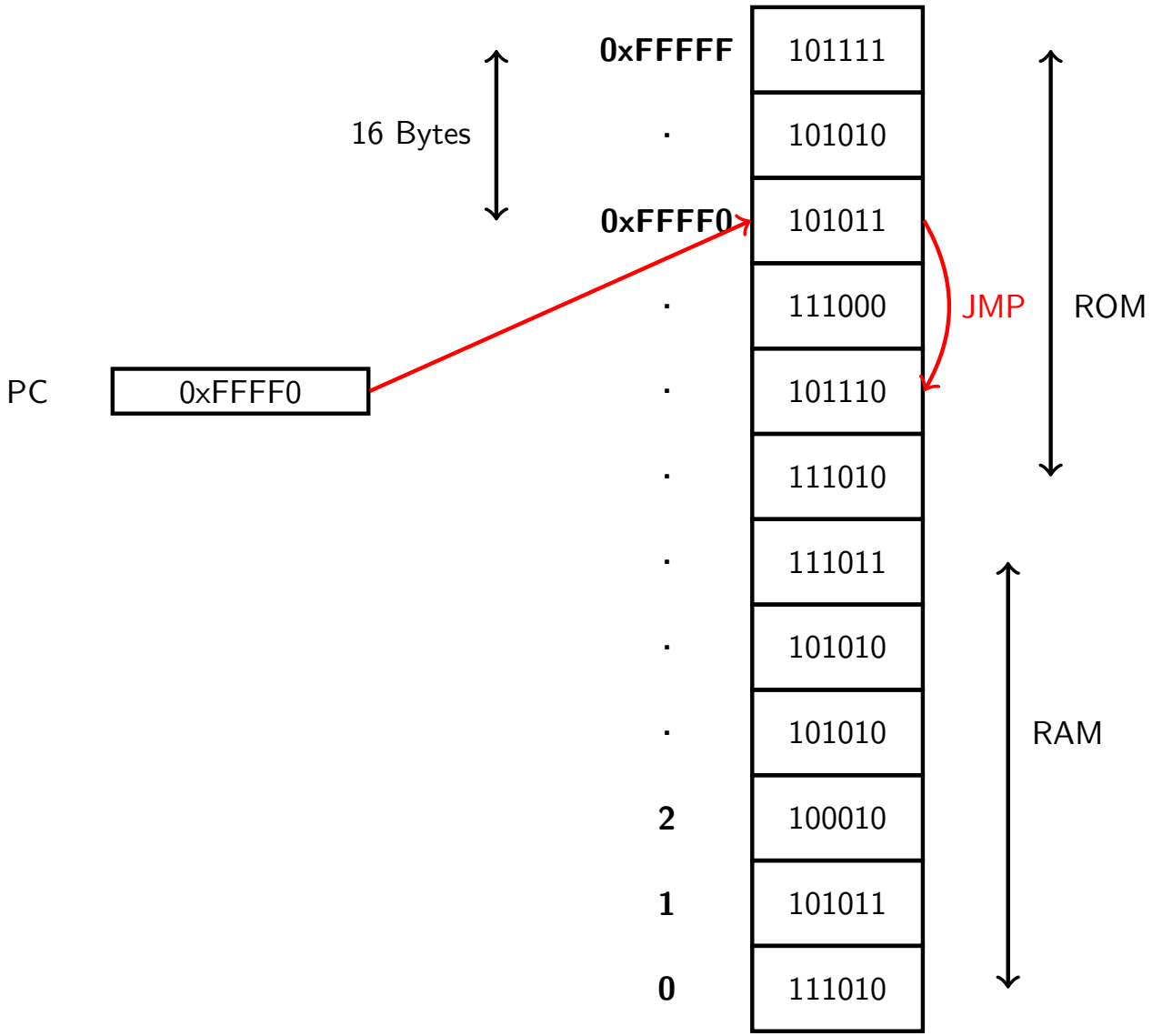
Write the following value (decimal) as a hexadecimal number.

$$2^{20} - 1$$


0xFFFFF
101111
101010
0xFFFF0
101011
111000
PC
0xFFFF0
101110
111010
111011
1 MB
101010
101010
2
100010
1
101011
0
111010

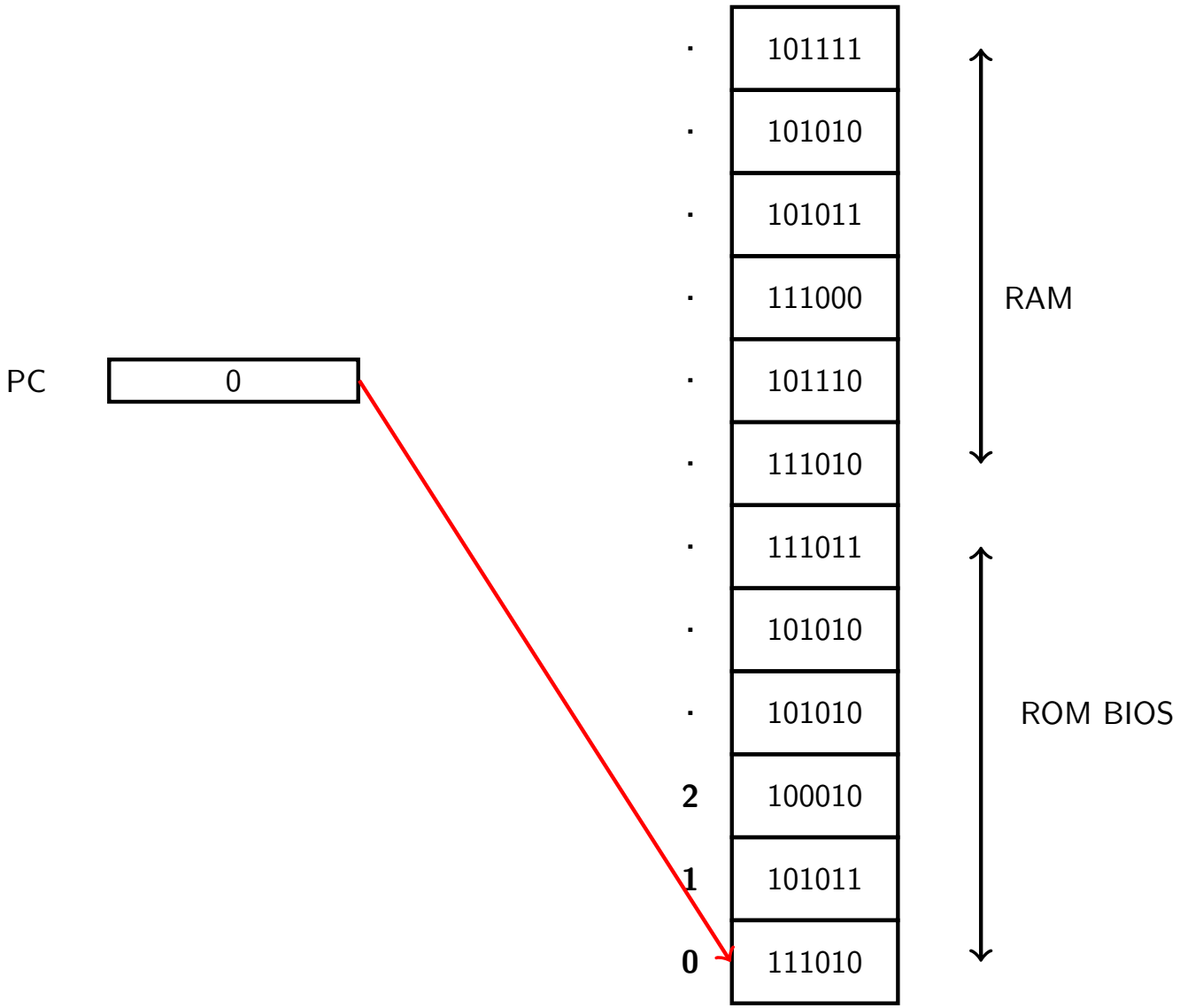

0xFFFFF
101111
101010
0xFFFF0
101011
111000
ROM
PC
0xFFFF0
101110
111010
111011
101010
101010
RAM
2
100010
1
101011
0
111010


16 Bytes
PC
0xFFFF0
0xFFFFF
0xFFFF0
101111
101010
101011
111000
101110
111010
111011
101010
101010
100010
101011
111010
2
1
0
ROM
RAM

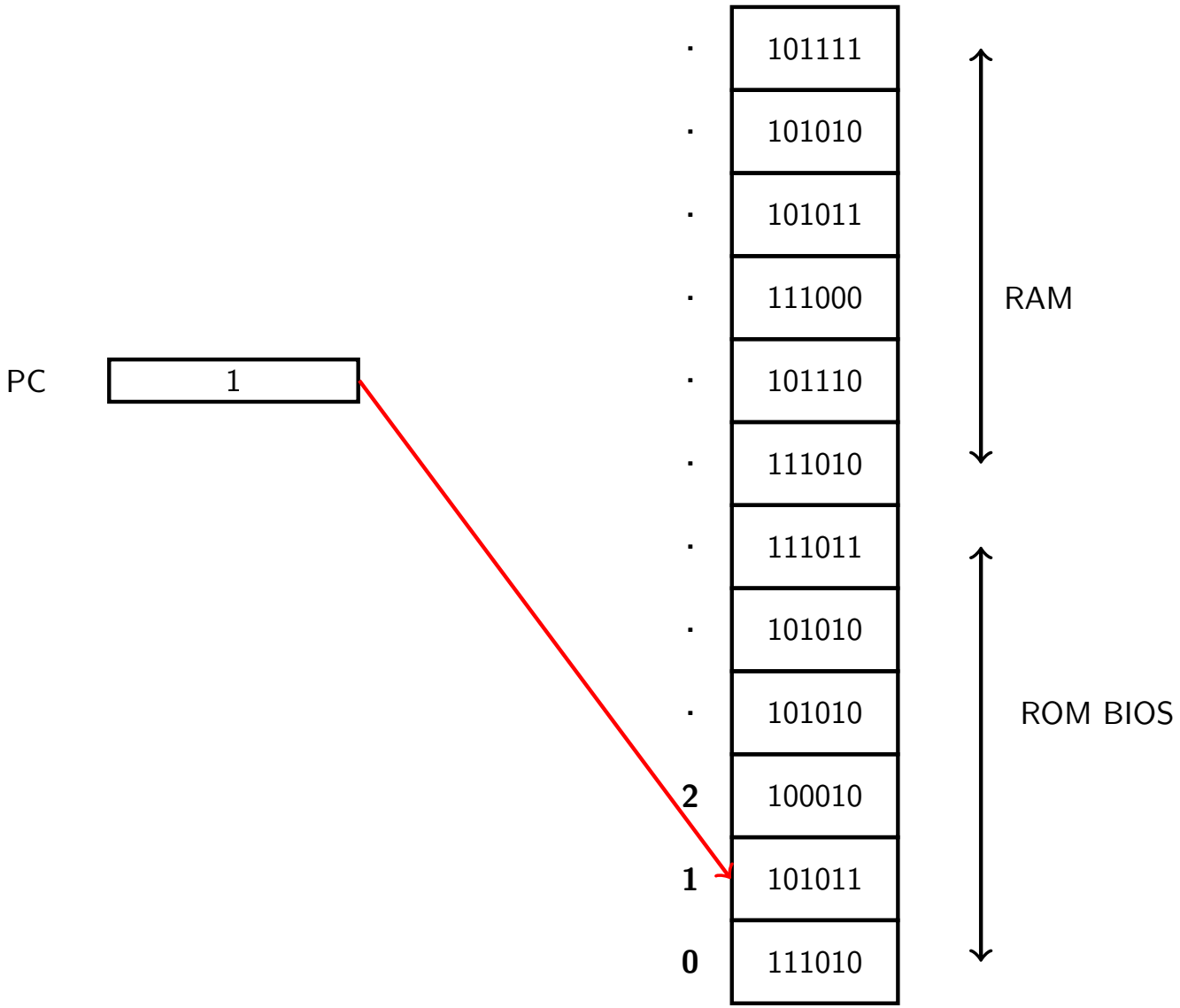

16 Bytes
0xFFFFF
0xFFFF0
PC
0xFFFF0
101111
101010
101011
111000
101110
111010
111011
101010
101010
100010
101011
111010
JMP
ROM
RAM
2
1
0

sudo cat /proc/iomem | grep ROM

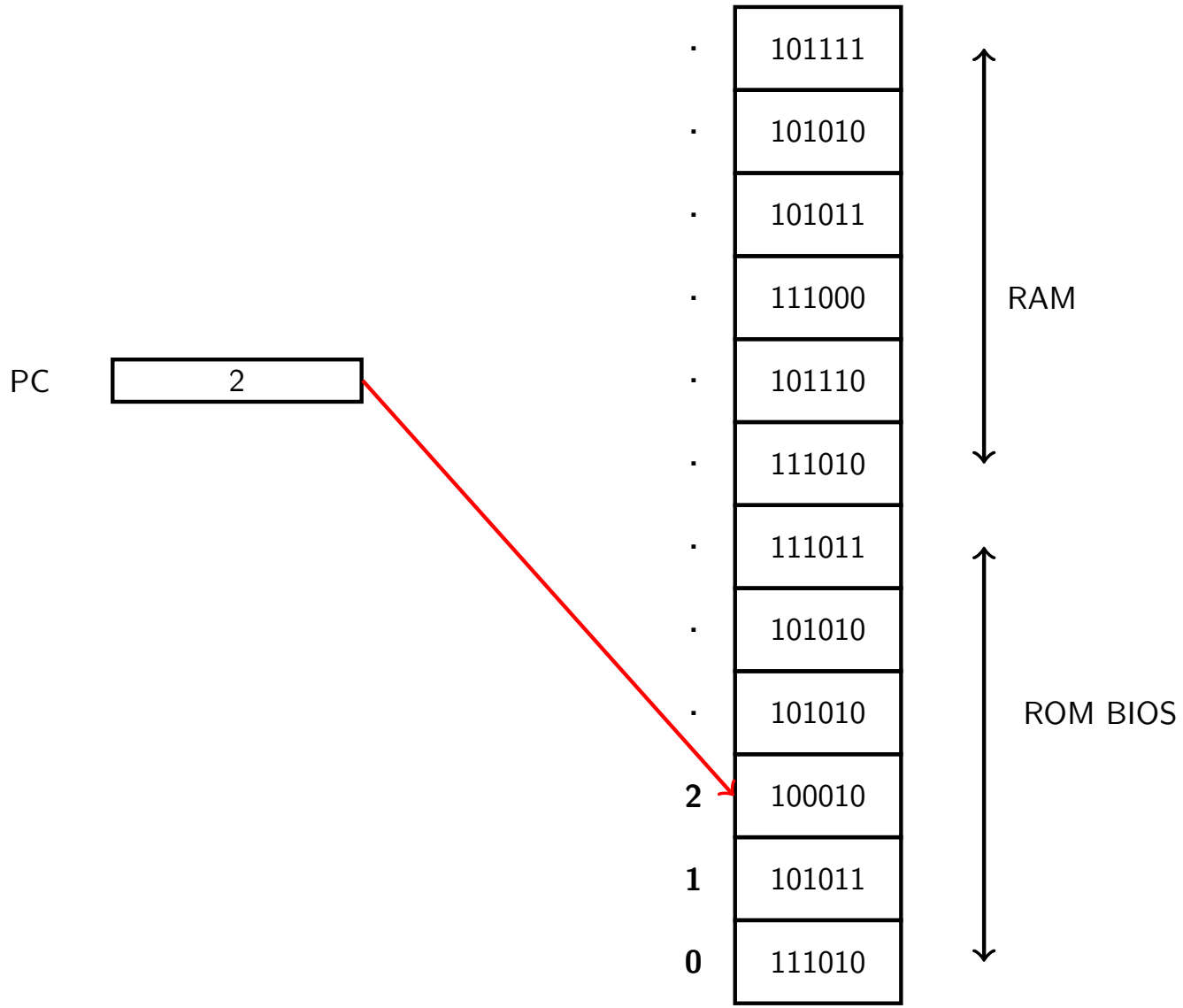
Basic Input Output System - BIOS



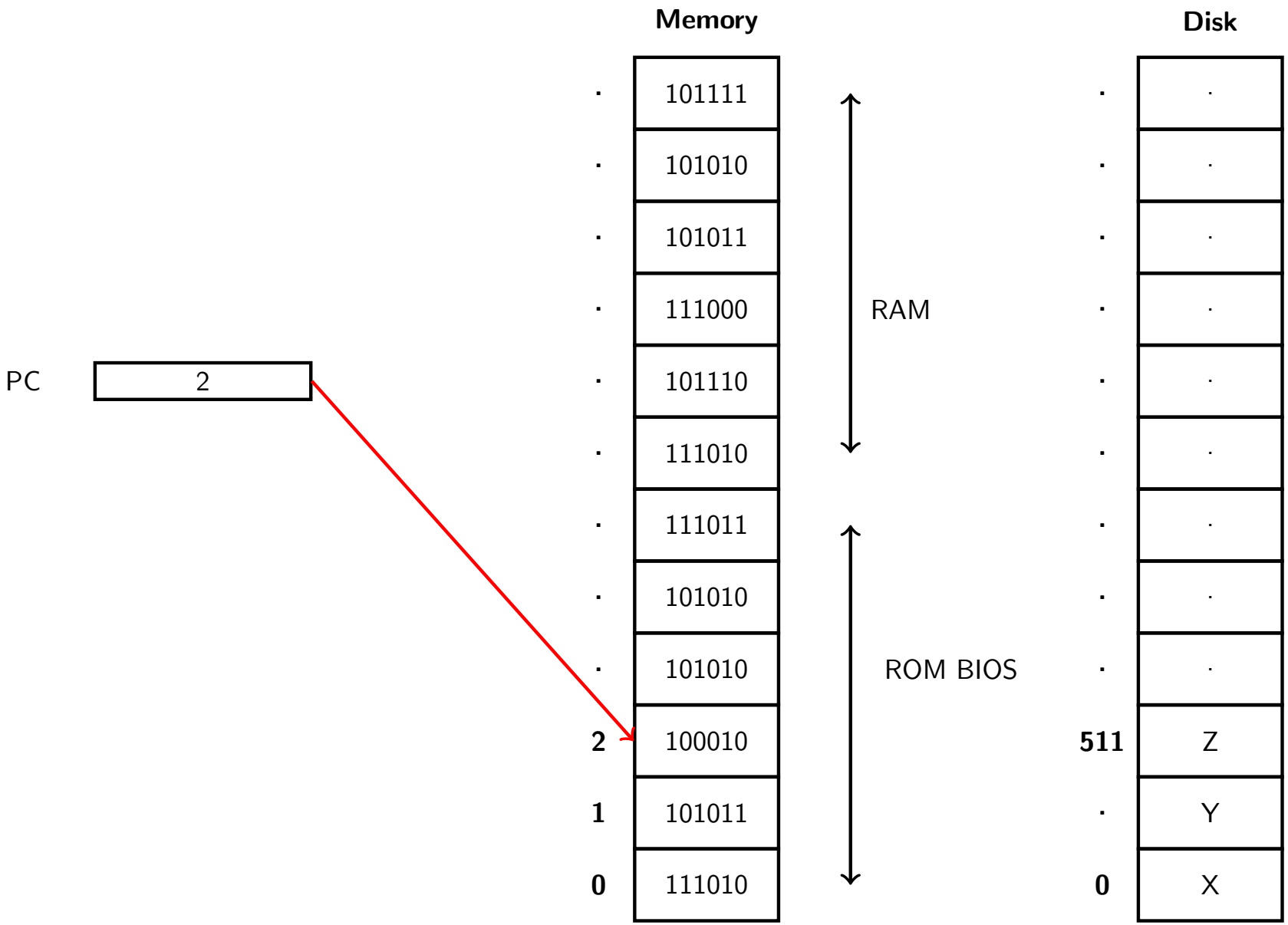
Basic Input Output System - BIOS



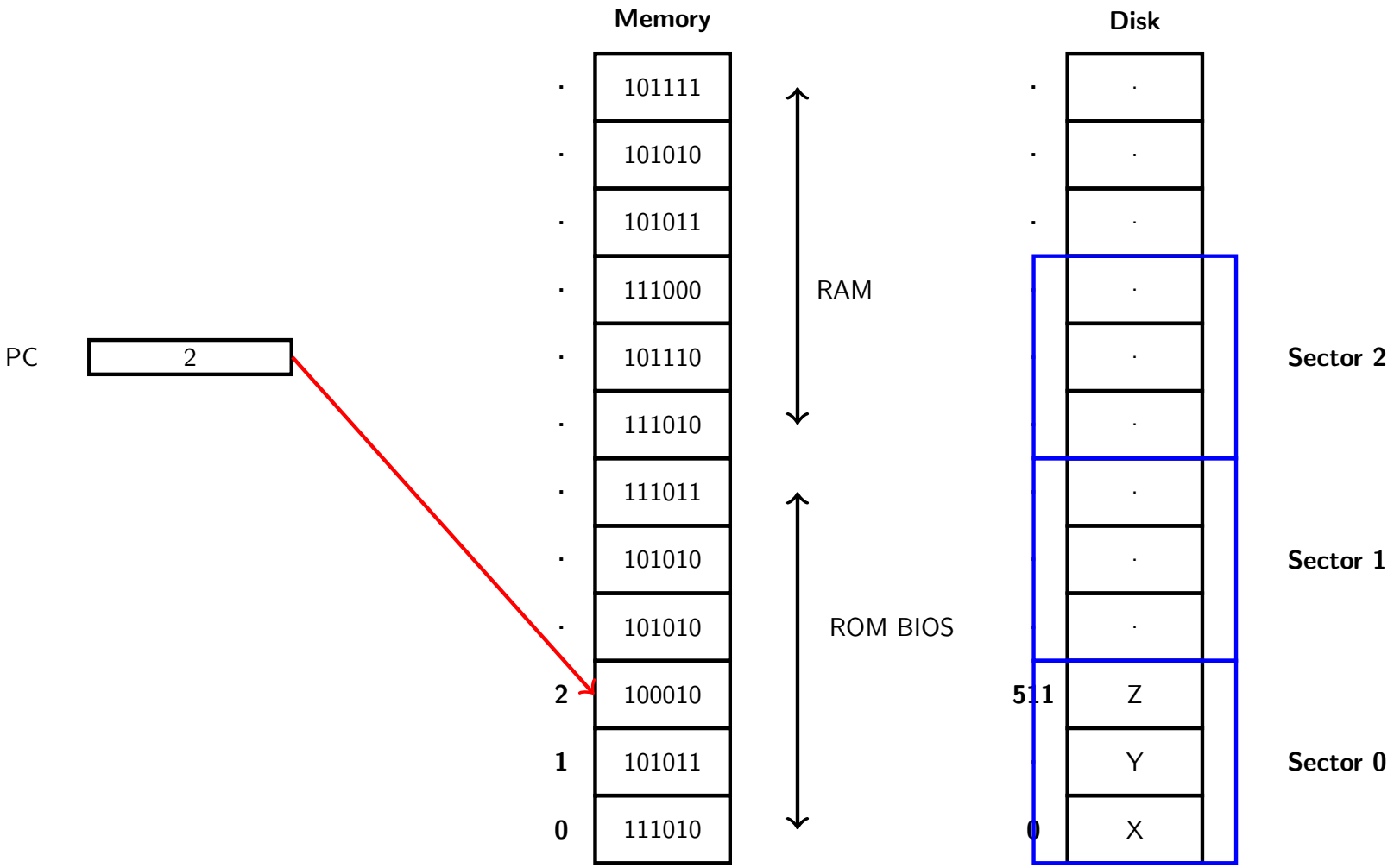
Basic Input Output System - BIOS



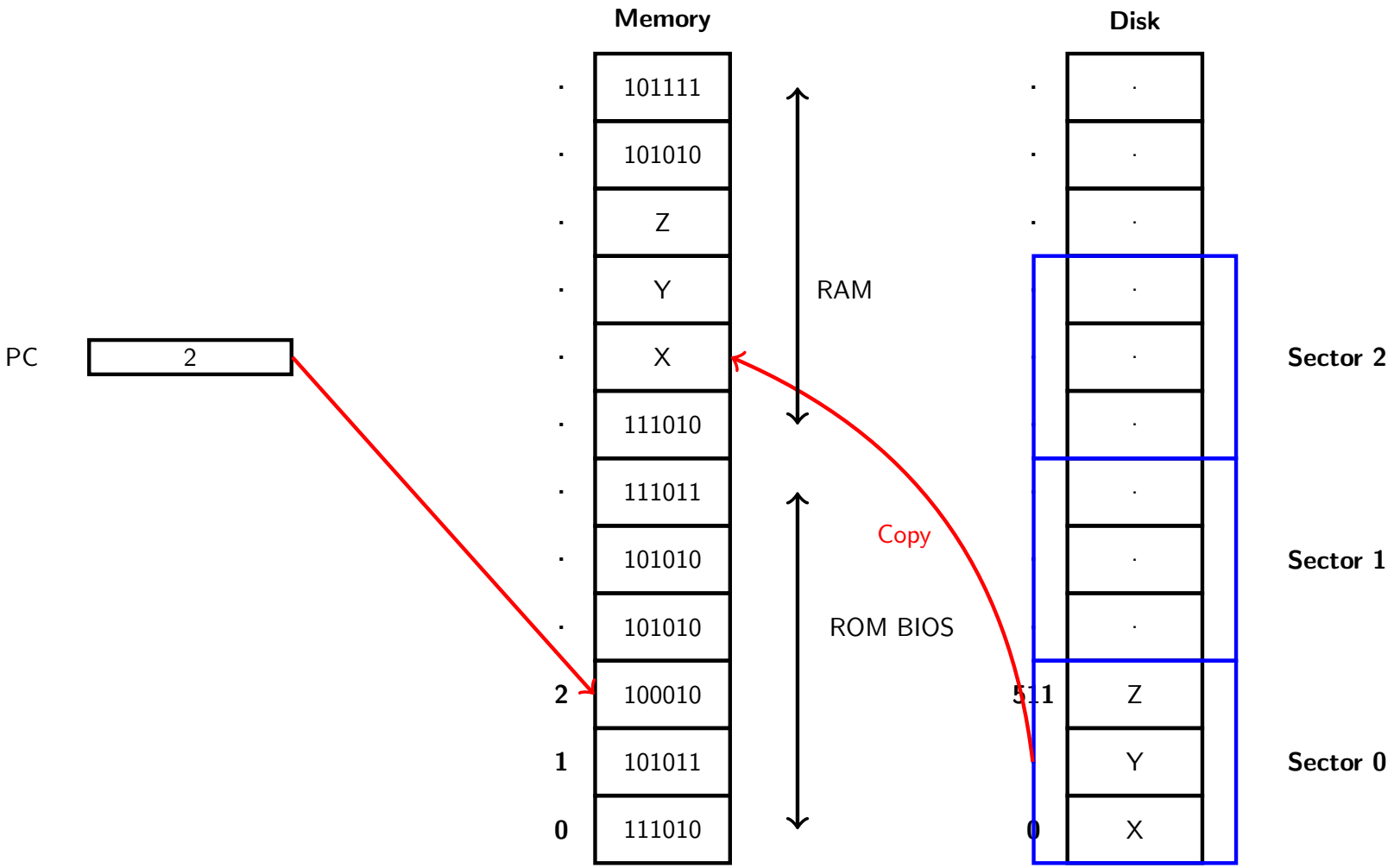
Basic Input Output System - BIOS



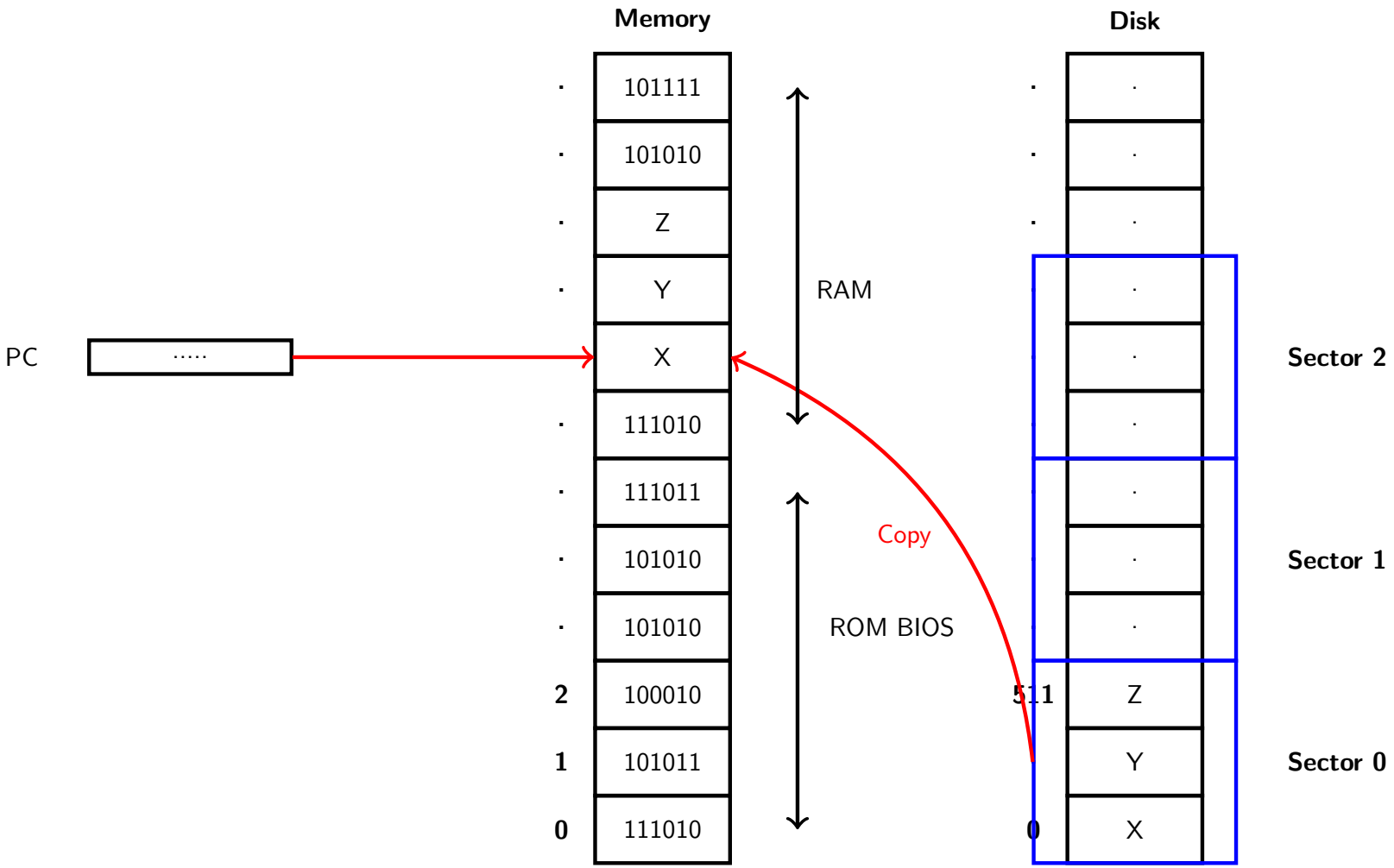
Basic Input Output System - BIOS



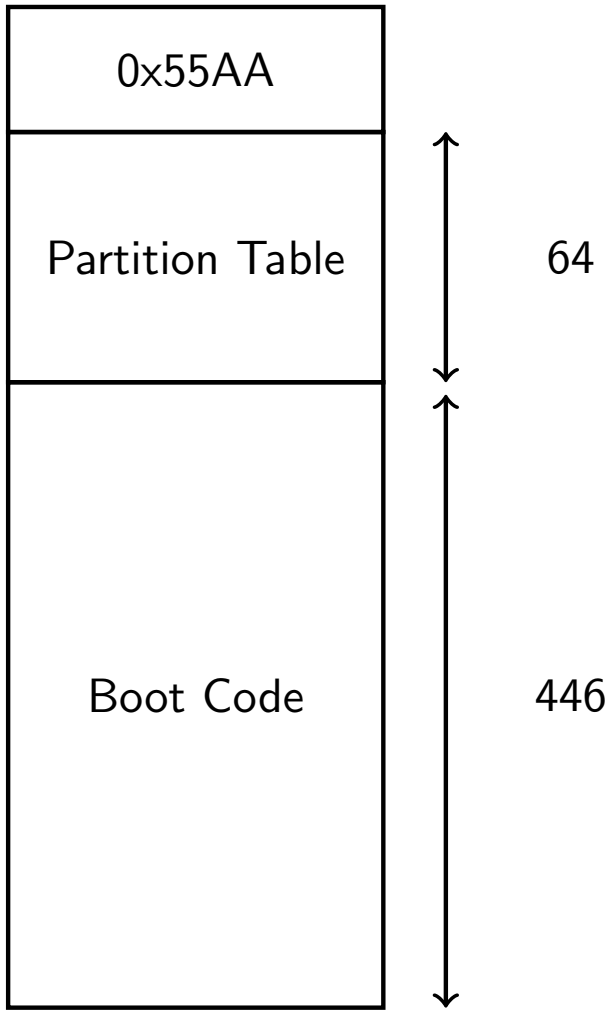
Basic Input Output System - BIOS



Basic Input Output System - BIOS

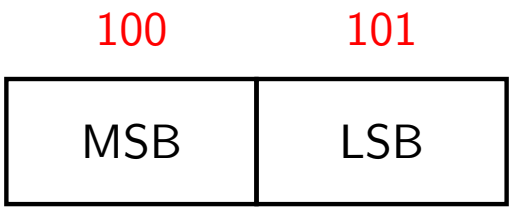


Master Boot Record

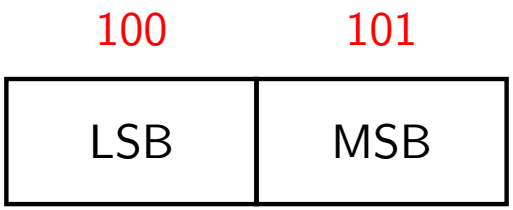


MSB and LSB

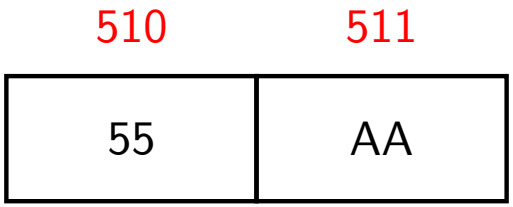
Big-Endian



Little-Endian

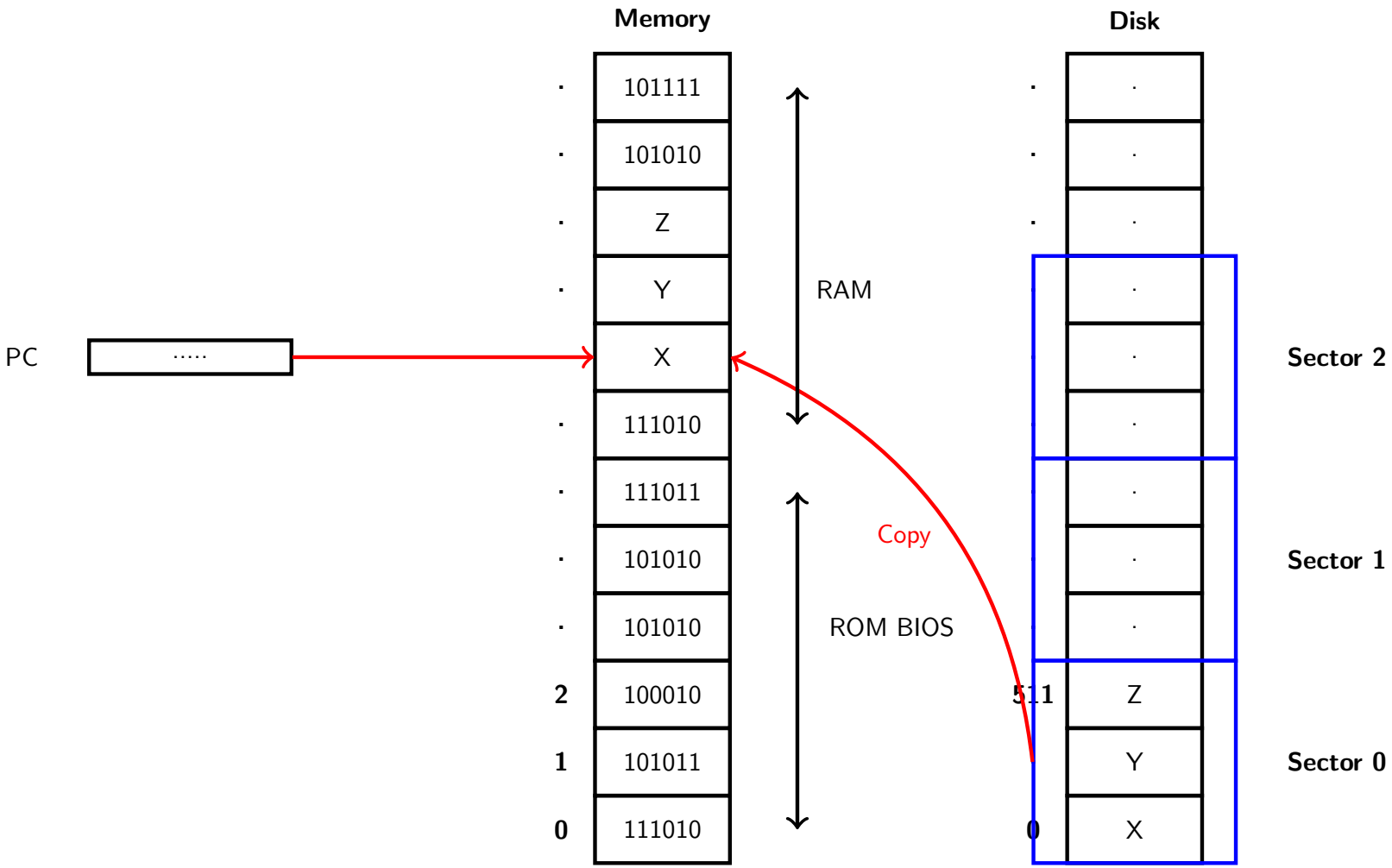


Little-Endian

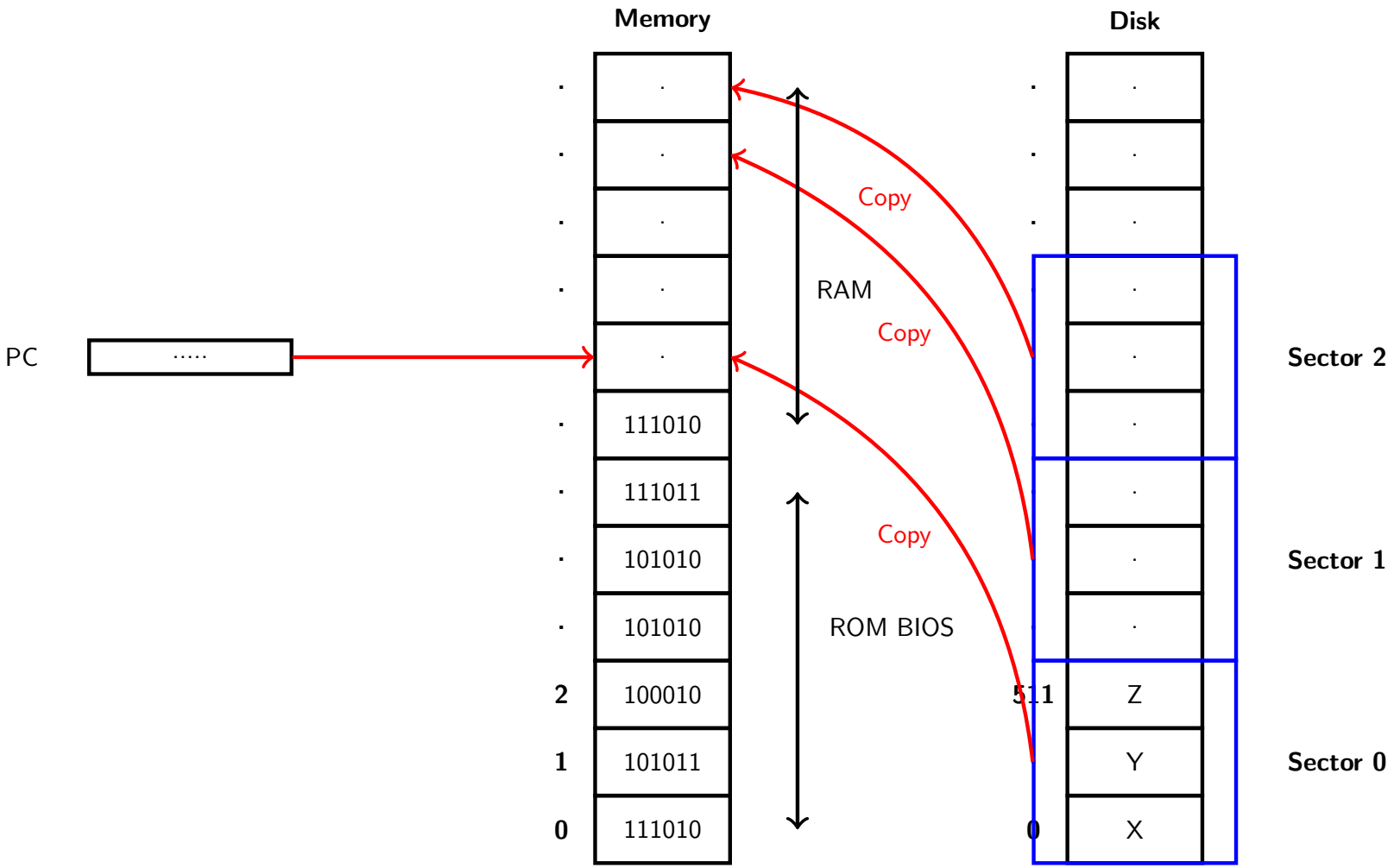


0xAA55

Booting


Memory
Disk
101111
101010
Z
Y
X
111010
111011
101010
101010
100010
101011
111010
RAM
ROM BIOS
PC
.....
Copy
2
1
0
511
0
Z
Y
X
Sector 2
Sector 1
Sector 0

Booting

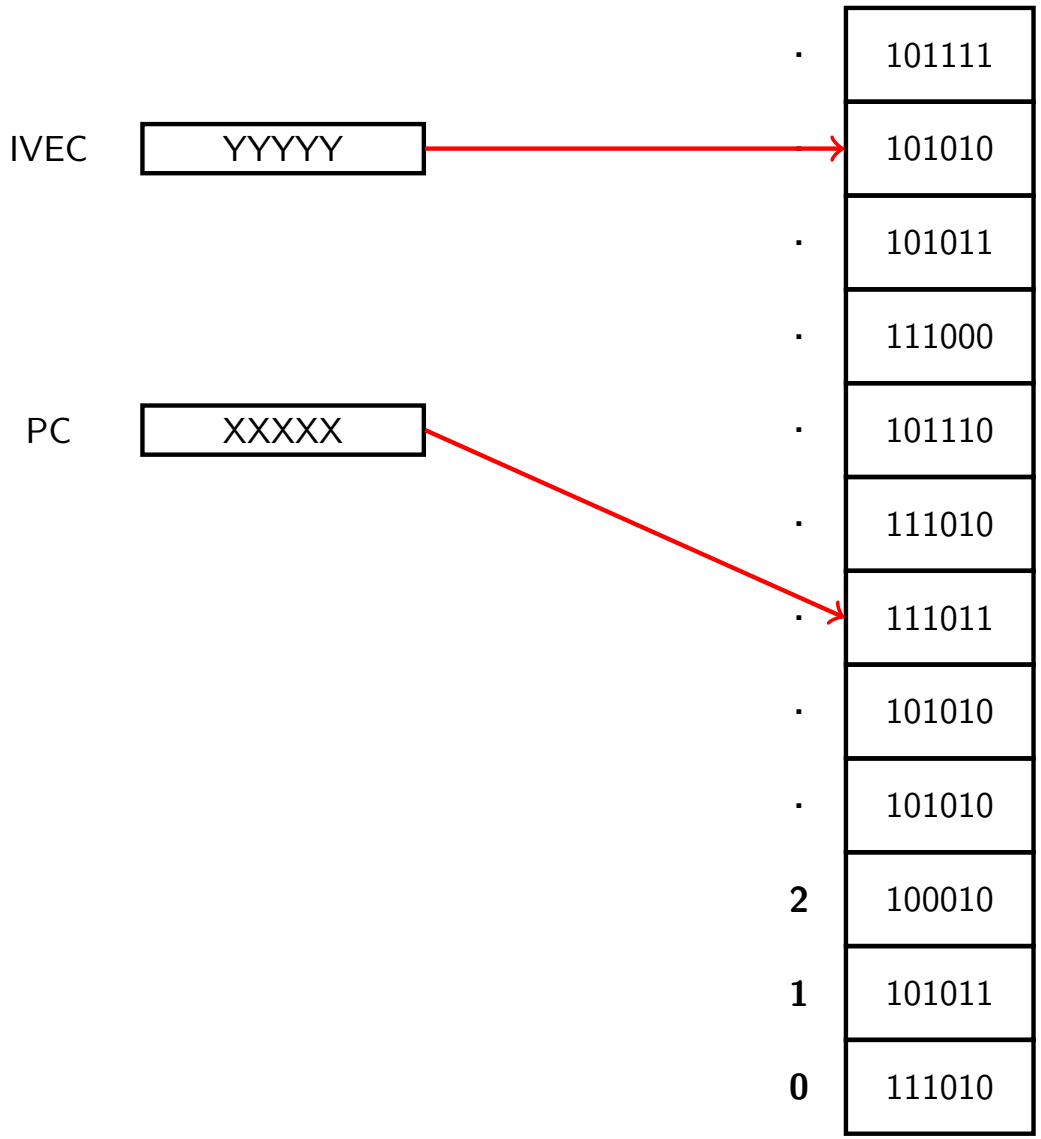

Memory
Disk
PC
.....
111010
111011
101010
101010
100010
101011
111010
RAM
ROM BIOS
Copy
Copy
Copy
2
1
0
511
0
Z
Y
X
Sector 2
Sector 1
Sector 0

Real Mode - Ring 0

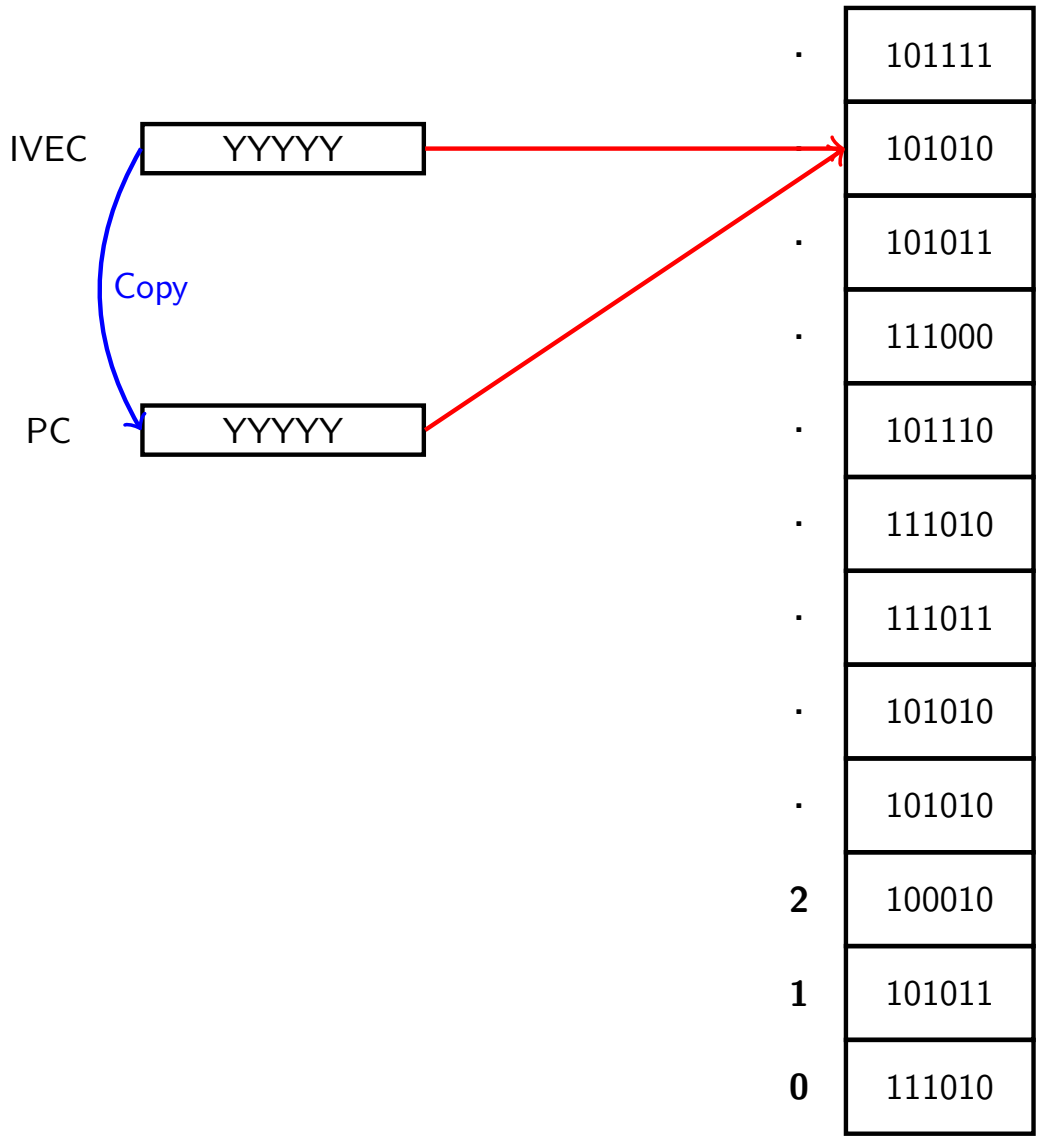
x86 - Interrupt Vector

Interrupt Descriptor Table Register (IDTR)

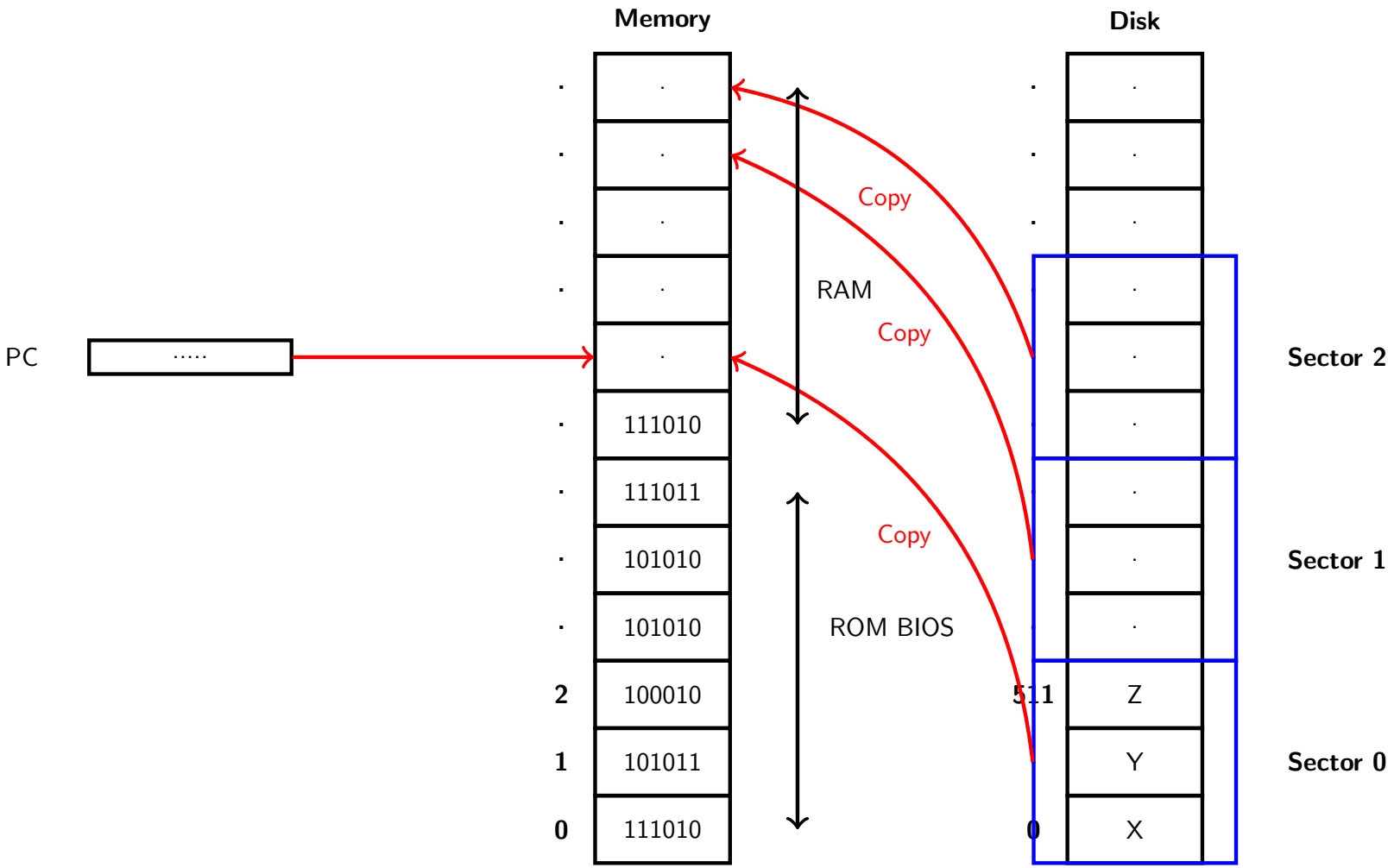
Interrupt Vector



Interrupt Vector



init/systemd First Userland Process - PID 1



f.c

```
int f()
{
// Some stuff here


   return 0;
}
```

f.s

```
f:
        movl  $20, %eax
        movl  $10, %ebx
        ....
        ....
        ret
```

main.c

```
int main(void)
{
// Some stuff here

   f();

// Some other stuff here
   return 0;
}
```

main.s

```
main:
        movl  $100, %eax
        movl  $125, %ebx
        ....
        ....
        call  _f
        addl   %eax, %ebx
        ...
        ...
        ...
```

Calling Functions