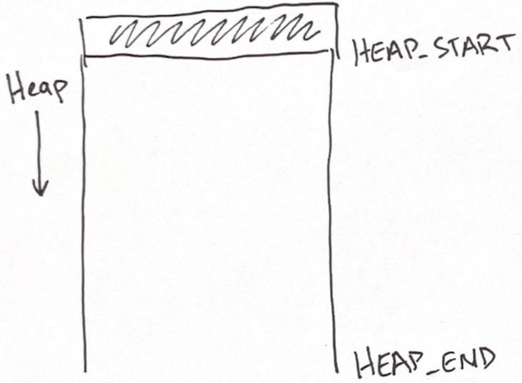
Malloc + free - how do they work?

They are C code



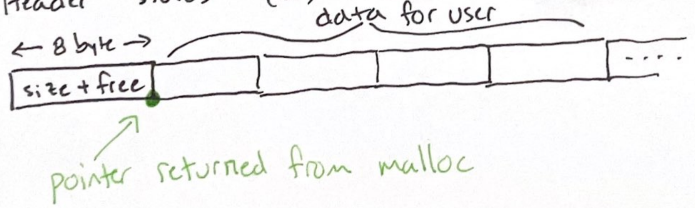
Key idea: on each malloc or free, store metadata about allocations

Metadata is stored on the heap.

Malloc will create "blocks" on the heap.

Each block will have a special first 8 bytes called "header"

Header stores (a) the size of the block (b) if block is free or "busy"
allocated



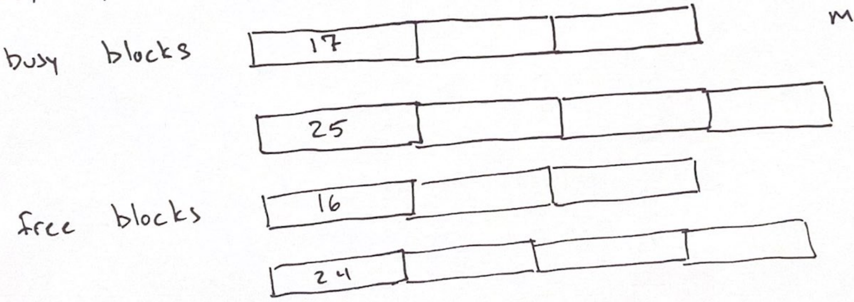
How to represent size + free in 8 bytes?

Invariant: all blocks start on a 8 byte boundary (all sizes are 8n)

so all sizes end in 000

Size is 64-bit unsigned number

Free/busy is the LSB = 1 ⇒ busy   LSB = 0 ⇒ free



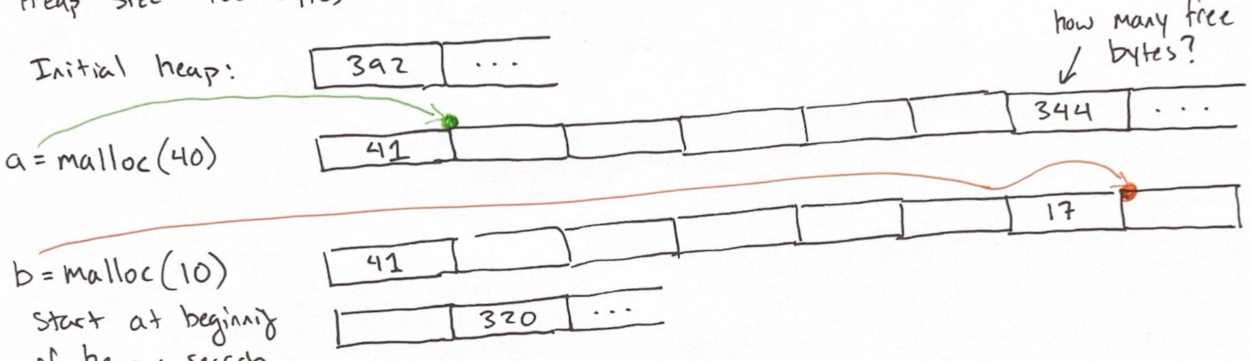
malloc (16)

malloc (20)

- round up to 24
- then write header 25

(side note: realloc(24) ought to be in-place)

Heap size 400 bytes



start at beginning of heap + search for free block